AVG Internet Security 2012

Manual do Usuário

Revisão do documento 2012.01 (1.9.2011)

Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.
Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

Este produto usa o RSA Data Security, Inc. Algoritmo de Compilador de Mensagem MD5, Copyright (C) 1991-2, RSA Data Security, Inc. Criado em 1991.
Este produto usa o código da biblioteca C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).
Este produto usa a biblioteca de compactação zlib, Copyright (c) 1995-2002 Jean-loup Gailly e Mark Adler.
Este produto usa a biblioteca de compactação libbzip2, Copyright (c) 1996-2002 Julian R. Seward.

Conteúdo

1. Introdução 7

2. Requisitos de instalação do AVG 8

2.1 Sistemas operacionais suportados 8
2.2 Requisitos de HW mínimos e recomendados 8

3. Processo de instalação do AVG 9

3.1 Bem-vindo 9
3.2 Ative a sua Licença 11
3.3 Selecionar tipo de instalação 12
3.4 Opções personalizadas 13
3.5 Instalar a Barra de Ferramentas de Segurança do AVG 15
3.6 Progresso da Instalação 16
3.7 Instalação bem sucedida 17

4. Após a instalação 19

4.1 Registro do produto 19
4.2 Acesso à interface do usuário 19
4.3 Verificação de todo o computador 19
4.4 Teste Eicar 19
4.5 Configuração padrão do AVG 20

5. Interface de usuário do AVG 21

5.1 Menu do sistema 22
5.1.1 Arquivo 22
5.1.2 Componentes 22
5.1.3 Histórico 22
5.1.4 Ferramentas 22
5.1.5 Ajuda 22
5.1.6 Suporte 22
5.2 Informações sobre status de segurança 29
5.3 Links rápidos 30
5.4 Visão geral dos componentes 31
5.5 Ícone da bandeja do sistema 33
5.6 Gadget AVG 34

6. Componentes do AVG 37

AVG Internet Security 2012 © 2011 Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.

6.1 Antivírus 37
6.1.1 Mecanismo de verificação 37
6.1.2 Proteção Residente 37
6.1.3 Proteção Anti-spyware 37
6.1.4 Interface do Antivírus 37
6.1.5 Detecções de Proteção Residente 37
6.2 Link Scanner 43
6.2.1 Interface do Link Scanner 43
6.2.2 Detecções do Search-Shield 43
6.2.3 Detecções do Surf-Shield 43
6.2.4 Detecções da Proteção Online 43
6.3 Proteção de E-mail 49
6.3.1 Verificador de E-mail 49
6.3.2 Anti-spam 49
6.3.3 Interface da Proteção de E-mail 49
6.3.4 Detecções da Proteção de E-mail 49
6.4 Firewall 53
6.4.1 Princípios do Firewall 53
6.4.2 Perfis do Firewall 53
6.4.3 Interface do Firewall 53
6.5 Anti-Rootkit 57
6.5.1 Interface do Anti-Rootkit 57
6.6 Ferramentas do Sistema 59
6.6.1 Processos 59
6.6.2 Conexões da Rede 59
6.6.3 Início automático 59
6.6.4 Navegador de Extensões 59
6.6.5 Visualizador LSP 59
6.7 PC Analyzer 65
6.8 Identity Protection 66
6.8.1 Interface da Proteção de Identidade 66
6.9 Administração Remota 69

7. Meus aplicativos 70

7.1 LiveKive 70
7.2 Family Safety 71
7.3 PC Tuneup 71

8. Barra de Ferramentas de Segurança do AVG 73

9. Configurações Avançadas do AVG 75

9.1 Aparência 75
9.2 Sons 78
9.3 Desativar temporariamente a proteção do AVG 79
9.4 Antivírus 81
9.4.1 Proteção Residente 81
9.4.2 Servidor de cache 81
9.5 Proteção de e-mail 86
9.5.1 Verificador de e-mail 86
9.5.2 Anti-Spam 86
9.6 Link Scanner 104
9.6.1 Configurações do Verificador de link 104
9.6.2 Proteção On-line 104
9.7 Verificações 108
9.7.1 Verificação de todo o computador 108
9.7.2 Verificação da extensão Shell 108
9.7.3 Verificação de arquivos ou pastas específicas 108
9.7.4 Verificação de dispositivo removível 108
9.8 Programações 114
9.8.1 Verificação programada 114
9.8.2 Agendamento de atualização de definições 114
9.8.3 Agendamento de atualização de programa 114
9.8.4 Agendamento de atualização do anti-spam 114
9.9 Atualizar 125
9.9.1 Proxy 125
9.9.2 Dial-up 125
9.9.3 URL 125
9.9.4 Gerenciar 125
9.10 Anti-Rootkit 132
9.10.1 Exceções 132
9.11 Identity Protection 133
9.11.1 Configurações do Identity Protection 133
9.11.2 Lista de permissões 133
9.12 Programas Potencialmente Indesejáveis 137
9.13 Quarentena de vírus 140
9.14 Programa de aprimoramento de produtos 140
9.15 Status ignorar erro 143

9.16 Administração Remota 144

10. Configurações de Firewall 146

10.1 Geral 146
10.2 Segurança 147
10.3 Perfis de áreas e adaptadores 148
10.4 IDS 149
10.5 Logs 151
10.6 Perfis 153
10.6.1 Informações do perfil 153
10.6.2 Redes definidas 153
10.6.3 Aplicativos 153
10.6.4 Serviços do sistema 153

11. Verificação do AVG 164

11.1 Interface da verificação 164
11.2 Verificações predefinidas 165
11.2.1 Verificação de todo o computador 165
11.2.2 Verificar arquivos ou pastas específicos 165
11.2.3 Verificação Anti-Rootkit 165
11.3 Verificando o Windows Explorer 175
11.4 Verificação de linha de comando 176
11.4.1 Parâmetros de verificação CMD 176
11.5 Programação de verificação 179
11.5.1 Configurações de programação 179
11.5.2 Como verificar 179
11.5.3 O que verificar 179
11.6 Visão geral dos resultados da verificação 188
11.7 Detalhes dos resultados da verificação 189
11.7.1 Guia Visão geral dos resultados 189
11.7.2 Guia Infecções 189
11.7.3 Guia Spyware 189
11.7.4 Guia Avisos 189
11.7.5 Guia Rootkits 189
11.7.6 Guia Informações 189
11.8 Quarentena de vírus 197

12. Atualizações do AVG 199

12.1 Iniciar atualização 199

12.2 Progresso da atualização 199
12.3 Níveis de atualização 200

13. Histórico de Eventos 202

14. Perguntas Freqüentes e Suporte Técnico 204

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG Internet Security 2012**.

O **AVG Internet Security 2012** fornece várias camadas de proteção para tudo o que você faz online. Isso significa que você não precisa se preocupar com roubos de identidade, vírus ou visitas a sites prejudiciais. Os recursos AVG Protective Cloud Technology e AVG Community Protection Network estão incluídos, o que significa que obtemos as informações sobre as ameaças mais recentes e as compartilhamos com nossa comunidade para garantir que você receba a melhor proteção:

- Faça compras e realize transações bancárias com segurança usando o Firewall AVG, o Anti-Spam e o Identity Protection
- Fique protegido em redes sociais com o AVG Social Networking Protection
- Navegue e pesquise com segurança utilizando a proteção em tempo real do LinkScanner

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais suportados

O **AVG Internet Security 2012** destina-se à proteção de estações de trabalho com os seguintes sistemas operacionais:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64,todas as edições)
- Windows 7 (x86 e x64, todas as edições)

(e possíveis service packs posteriores para sistemas operacionais específicos)

***Observação**: o componente ID Protection não é suportado no Windows e XP x64. Nesses sistemas operacionais, é possível instalar AVG Internet Security 2012, mas sem o componente IDP.*

2.2. Requisitos de HW mínimos e recomendados

Requisitos mínimos de hardware para **AVG Internet Security 2012**:

- CPU Intel Pentium 1,5 GHz
- 512 MB de memória RAM
- 1.000 MB de espaço livre em disco rígido (para fins de instalação)

Requisitos recomendados de hardware para **AVG Internet Security 2012**:

- CPU Intel Pentium 1,8 GHz
- 512 MB de memória RAM
- 1.550 MB de espaço livre em disco rígido (para fins de instalação)

3. Processo de instalação do AVG

Onde posso obter o arquivo de instalação?

Para instalar o **AVG Internet Security 2012** em seu computador, você precisa obter o arquivo de instalação mais recente. Para garantir que você esteja instalando a versão atualizada do **AVG Internet Security 2012**, recomenda-se baixar o arquivo de instalação no site do AVG (http://www.avg.com/). A seção ***Centro de Suporte/Download*** fornece uma visão geral estruturada dos arquivos de instalação para cada edição do AVG.

Se você não tiver certeza de quais arquivos precisa baixar e instalar, poderá usar o serviço ***Selecionar produto*** na parte inferior da página da Web. Depois que você responder a três simples perguntas, o serviço definirá exatamente os arquivos de que precisa. Clique no botão ***Continuar*** para ser redirecionado a uma lista completa de arquivos para download que foram personalizados para suas necessidades.

Como ocorre o processo de instalação?

Depois de fazer download e salvar o arquivo de instalação no disco rígido, você poderá iniciar o processo de instalação. A instalação é uma sequência de caixas de diálogo simples e fáceis de entender. Cada caixa de diálogo oferece uma rápida descrição de como proceder em cada etapa do processo de instalação. A seguir, oferecemos uma explicação detalhada sobre cada janela de caixa de diálogo:

3.1. Bem-vindo

O processo de instalação é iniciado com a caixa de diálogo ***Bem-vindo ao Instalador do AVG***:

Selecione o idioma do aplicativo

Nesta caixa de diálogo, você pode selecionar o idioma usado para o processo de instalação. No canto inferior direito da caixa de diálogo, clique na caixa de combinação para percorrer o menu de idiomas. Selecione o idioma desejado, e o processo de instalação continuará no idioma de sua escolha.

Atenção: no momento, você está somente selecionando o idioma do processo de instalação. O aplicativo AVG Internet Security 2012 será instalado no idioma selecionado e em inglês, que é sempre instalado automaticamente. No entanto, é possível ter mais idiomas instalados e trabalhar com o AVG Internet Security 2012 em qualquer um desses. Você será solicitado a confirmar a seleção completa dos idiomas alternativos em uma das seguintes caixas de diálogo de configuração Opções personalizadas.

Contrato de licença

Além disso, a caixa de diálogo ***Bem-vindo ao Instalador do AVG*** fornece a versão completa do contrato de licença do AVG. Leia-o com atenção. Para confirmar que leu, compreendeu e aceita o contrato, pressione o botão ***Aceitar***. Se você não concordar com o contrato de licença, pressione o botão Recusar e o processo de instalação será encerrado imediatamente.

Política de Privacidade do AVG

Além do contrato de licença, esta caixa de diálogo de configuração oferece a opção para você saber mais sobre a política de privacidade do AVG. No canto inferior esquerdo da caixa de diálogo, você pode ver o link ***Política de Privacidade do AVG***. Clique nele para ser redirecionado ao site do AVG (http://www.avg.com/), onde você pode encontrar todos os princípios da política de privacidade da AVG Technologies.

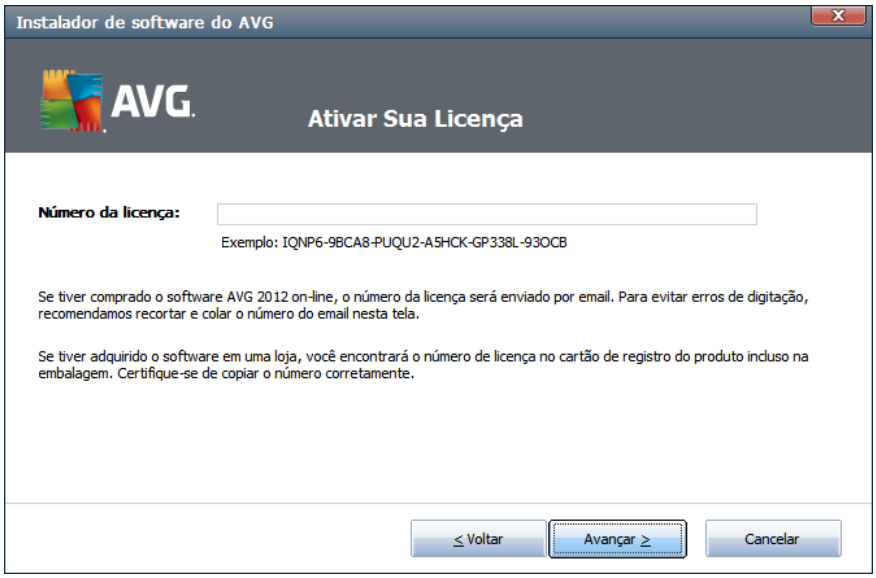
Botões de controle

Na primeira caixa de diálogo de instalação, há somente dois botões de controle disponíveis:

- ***Aceitar*** - clique para confirmar que você leu, compreendeu e aceitou o contrato de licença. A instalação continuará e você avançará para a próxima caixa de diálogo de configuração.
- ***Recusar*** - clique para recusar o contrato de licença. O processo de configuração será encerrado imediatamente. **AVG Internet Security 2012** não será instalado!

3.2. Ative a sua Licença

Na caixa de diálogo ***Ativar sua Licença***, você deverá fornecer o número da sua licença no campo de texto fornecido:



Onde encontrar o número de licença

O número de vendas pode ser encontrado na embalagem do CD na caixa do **AVG Internet Security 2012**. O número da licença está no e-mail de confirmação recebido depois da aquisição do AVG Internet Security 2012 **on-line.** Digite o número exatamente como mostrado. Se o formulário digital do número de licença estiver disponível (*no e-mail*), é recomendável usar o método de copiar e colar para inseri-lo.

Como usar o método de copiar e colar.

O uso do método de ***copiar e colar*** para inserir seu número de licença do **AVG Internet Security 2012** no programa garante que o número seja inserido corretamente. Por favor siga esses passos:

- Abra o e-mail que contém o número de licença.
- Clique com o botão esquerdo do mouse no início do número de licença e mantenha o botão pressionando, arraste o mouse até o final do número e solte o botão. O número deverá estar realçado.
- Mantenha pressionada a tecla ***Ctrl*** enquanto pressiona a tecla ***C***. Desse modo, o número é copiado.
- Aponte e clique no local em que você deseja colar o número copiado.

- Mantenha pressionada a tecla ***Ctrl*** enquanto pressiona a tecla ***V***. Desse modo, o número é colado no local selecionado.

Botões de controle

Como a maioria das caixas de diálogo de instalação, há três botões de controle disponíveis.

- ***Voltar*** - clique para voltar à caixa de diálogo de instalação anterior.
- ***Avançar*** - clique para continuar a instalação e avançar uma etapa.
- ***Cancelar*** - clique para sair do processo de instalação imediatamente. O **AVG Internet Security 2012** não será instalado!

3.3. Selecionar tipo de instalação

Tipos de instalação

A caixa de diálogo ***Selecionar tipo de instalação*** oferece duas opções de instalação: ***Instalação Rápida*** e ***Instalação Personalizada***.

Para a maioria dos usuários, é altamente recomendável manter a opção Instalação Rápida ***padrão***, que instala o **AVG Internet Security 2012** no modo totalmente automático, com configurações predefinidas pelo fornecedor do programa. Essa configuração fornece o máximo de segurança combinado com o uso ideal dos recursos. No futuro, se houver necessidade de alterar a configuração, você sempre terá a possibilidade de fazer isso diretamente no aplicativo **AVG Internet Security 2012**. Se você tiver selecionado a opção ***Instalação Rápida***, pressione o botão ***Próximo*** para avançar para a caixa de diálogo Instalar a Barra de Ferramentas de Segurança do AVG seguinte.

A instalação personalizada deve ser usada somente por usuários experientes que tenham um motivo válido para instalar o **AVG Internet Security 2012** com configurações diferentes do padrão, como para atender aos requisitos específicos do sistema. Após selecionar esta opção, pressione o botão ***Próximo*** para avançara para a caixa de diálogo Opções Personalizadas.

Instalação do gadget do AVG

Na seção direita da caixa de diálogo, você pode encontrar a caixa de seleção relacionada ao gadget AVG (*com suporte no Windows Vista/Windows 7*). Se quiser instalar esse gadget, marque a respectiva caixa de seleção. O gadget AVG poderá ser acessado pela barra lateral do Windows, proporcionando-lhe um acesso imediato aos recursos mais importantes do seu **AVG Internet Security 2012**, por exemplo, verificação e atualização.

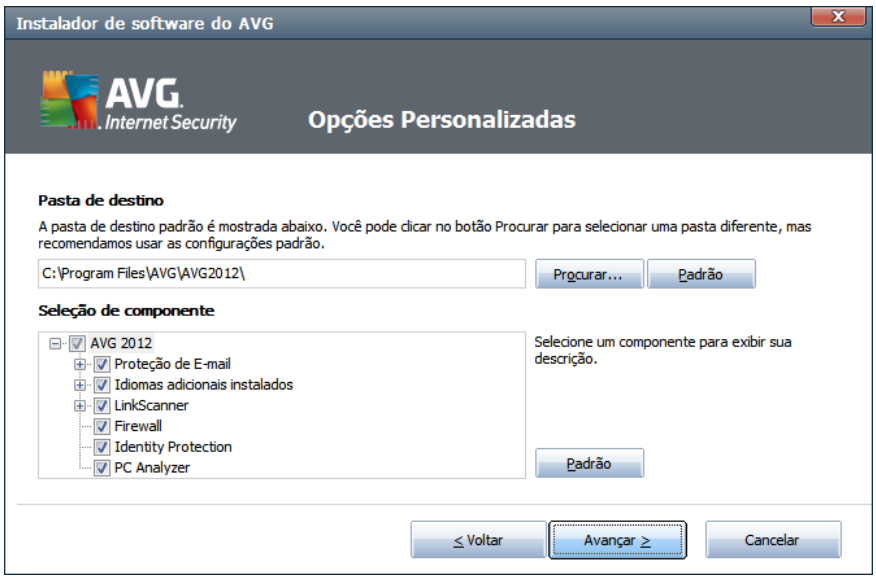
Botões de controle

Como a maioria das caixas de diálogo de instalação, há três botões de controle disponíveis.

- ***Voltar*** - clique para voltar à caixa de diálogo de instalação anterior.
- ***Avançar*** - clique para continuar a instalação e avançar uma etapa.
- ***Cancelar*** - clique para sair do processo de instalação imediatamente. O **AVG Internet Security 2012** não será instalado!

3.4. Opções personalizadas

A caixa de diálogo ***Opções Personalizadas*** permite configurar dois parâmetros da instalação:



Pasta de destino

Na seção ***Pasta de Destino*** da caixa de diálogo, você deve especificar o local onde o **AVG Internet Security 2012** deve ser instalado. Por padrão, o **AVG Internet Security 2012** será instalado na pasta de arquivos de programa localizada na unidade C:. Se você desejar alterar esse local, use o botão ***Procurar*** para exibir a estrutura da unidade e selecionar a respectiva pasta.

Seleção de componente

A seção ***Seleção de Componente*** exibe uma visão geral de todos os componentes **AVG Internet Security 2012** que podem ser instalados. Se as configurações padrão não forem adequadas a você, será possível remover/adicionar componentes específicos.

Entretanto, só é possível selecionar os componentes incluídos na edição do AVG que você adquiriu!

Selecione qualquer item na lista ***Seleção de Componente***, e uma breve descrição do respectivo componente será exibida no lado direito desta seção. Para informações detalhadas sobre a funcionalidade de cada componente, consulte o capítulo Visão Geral de Componentes dessa documentação. Para reverter para a configuração padrão predefinida pelo fornecedor do software, use o botão ***Padrão***.

Botões de controle

Assim como na maioria das caixa de diálogo, há três botões de controle disponíveis:

- ***Voltar*** - clique para voltar à caixa de diálogo de configuração anterior.
- ***Avançar*** - clique para continuar a instalação e avançar uma etapa.
- ***Cancelar*** - clique para sair do processo de configuração imediatamente. O **AVG Internet Security 2012** não será instalado.

3.5. Instalar a Barra de Ferramentas de Segurança do AVG

Na caixa de diálogo ***Instalar a Barra de Ferramentas de Segurança AVG***, decida se deseja instalar a Barra de Ferramentas de Segurança AVG. Se você não alterar as configurações padrão, esse componente será instalado automaticamente no navegador da Internet (*os navegadores suportados no momento são Microsoft Internet Explorer v. 6.0 ou mais recente e Mozilla Firefox v. 3.0 e mais recente*), para fornecer proteção online abrangente enquanto você estiver navegando pela Internet.

Além disso, você tem a opção de decidir se quer escolher o *AVG Secure Search (powered by Google)* como o provedor de pesquisa padrão. Em caso afirmativo, mantenha a respectiva caixa de seleção marcada.

3.6. Progresso da Instalação

A caixa de diálogo ***Progresso da Instalação*** mostra o andamento do processo de instalação e não requer intervenção:

Após a conclusão do processo de instalação, você será redirecionado automaticamente à próxima caixa de diálogo.

Botões de controle

Nesta caixa de diálogo, há somente um botão de controle disponível: ***Cancelar***. Este botão deve ser usado somente se você desejar interromper o processo de instalação. Nesse caso, o **AVG Internet Security 2012** não será instalado.

3.7. Instalação bem sucedida

A caixa de diálogo ***Instalação realizada com êxito*** confirma que o **AVG Internet Security 2012** foi totalmente instalado e configurado:

Programa de aprimoramento de produtos

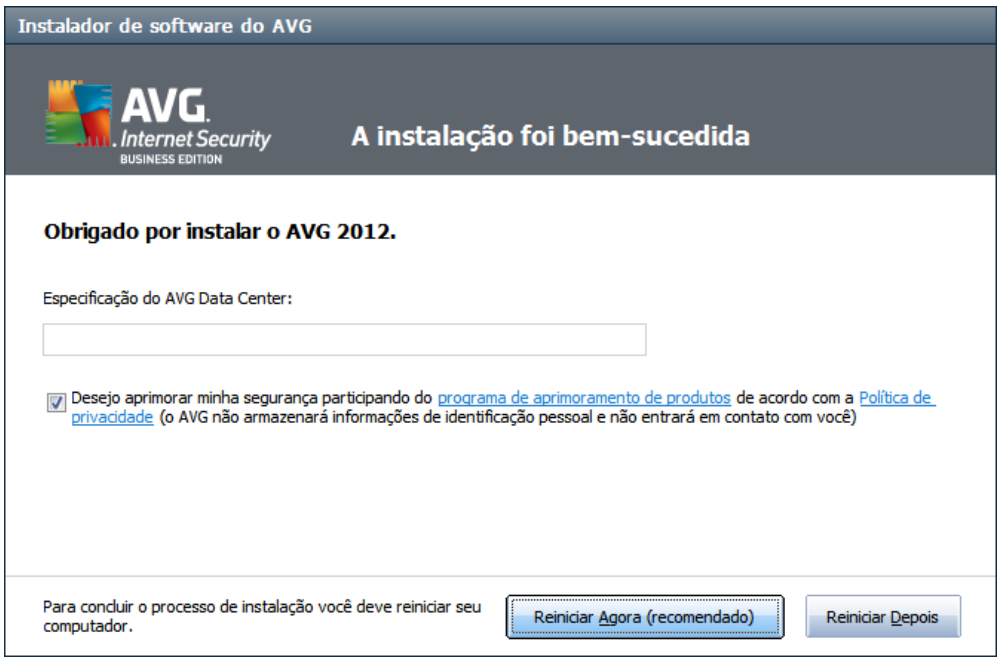
Nesta caixa de diálogo, você pode optar por participar do Programa de Aprimoramento de Produto (*para obter os detalhes, consulte o capítulo Configurações Avançadas do AVG/Programa de Aprimoramento de Produto*), que coleta informações anônimas sobre ameaças detectadas para aumentar o nível geral de segurança na Internet. Se você concordar com esta declaração, mantenha selecionada a opção ***Concordo em participar do Programa de Aprimoramento de Produto e Segurança na Web do AVG 2012...*** *(a opção é confirmada por padrão)*.

Reinicialização do computador

Para finalizar o processo de instalação, é preciso reiniciar o computador: selecione se deseja ***Reiniciar Agora*** ou adiar essa ação - ***Reiniciar Depois***.

Instalação da licença comercial

Se você estiver usando alguma licença comercial do AVG e caso tenha optado por instalar anteriormente o item Administração Remota *(consulte Opções Personalizadas)*, a caixa de diálogo Instalação bem-sucedida será exibida com a seguinte interface:



É preciso especificar os parâmetros do AVG DataCenter - forneça a string de conexão para o AVG DataCenter, no formato servidor:porta. Se essas informações não estiverem disponíveis no momento, deixe o campo em branco, e você poderá definir a configuração mais tarde, na caixa de diálogo Configurações avançadas / Administração remota. Para obter informações detalhadas sobre a Administração Remota do AVG, consulte o manual de usuário do AVG Business Edition, que pode ser baixado no site do AVG (http://www.avg.com/).

consulte o capítulo Visão geral dos componentes desta documentação. Para reverter para a configuração padrão predefinida pelo fornecedor do software, use o botão ***Padrão***.

Botões de controle

Na caixa de diálogo, os seguintes botões de controle estão disponíveis:

- ***Reiniciar Agora (recomendado)*** - a reinicialização é necessária para concluir o processo de instalação do **AVG Internet Security 2012**. É recomendado reiniciar o computador imediatamente. Somente após a reinicialização, o **AVG Internet Security 2012** estará totalmente instalado, e você ficará seguro e protegido.
- ***Reiniciar Depois*** - se, por algum motivo, você não puder reiniciar o computador agora, a ação poderá ser adiada para mais tarde. No entanto, recomenda-se reiniciá-lo imediatamente. Somente após a reinicialização, o **AVG Internet Security 2012** poderá proporcionar proteção total ao seu computador!

4. Após a instalação

4.1. Registro do produto

Quando a instalação do **AVG Internet Security 2012** for concluída, registre seu produto online no site do AVG (http://www.avg.com/). Depois do registro, você terá acesso completo à sua conta de usuário do AVG, ao boletim informativo de atualização do AVG e a outros serviços fornecidos exclusivamente para usuários registrados.

A forma mais fácil de registrar o produto é diretamente pela interface de usuário do **AVG Internet Security 2012**. No menu principal, selecione o item Ajuda/Registrar agora. Você será direcionado à página de ***Registro*** no site do AVG (http://www.avg.com/). Siga as instruções fornecidas na página.

4.2. Acesso à interface do usuário

A caixa de diálogo principal do AVG pode ser acessada de várias maneiras:

- clique duas vezes no ícone da bandeja de sistema do AVG
- clique duas vezes no ícone do AVG na área de trabalho
- clique duas vezes na linha de status localizada na seção inferior do gadget AVG (*se instalado; com suporte no Windows Vista/ Windows 7*)
- no menu ***Iniciar/Programas/AVG 2012/Interface do Usuário do AVG***

4.3. Verificação de todo o computador

Existe um risco potencial de um vírus de computador ter sido transmitido ao seu computador antes da instalação do **AVG Internet Security 2012** . Por esse motivo, você deve executar uma verificação de todo o computador para assegurar que seu PC não esteja infectado.

Para obter instruções sobre a Verificação em todo o computador, consulte o capítulo Verificação do AVG.

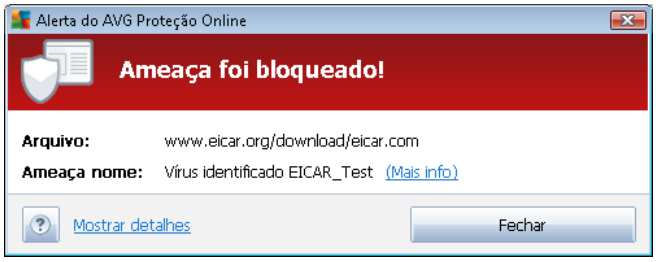
4.4. Teste Eicar

Para confirmar que **AVG Internet Security 2012** foi instalado corretamente, você pode executar o teste EICAR.

O teste EICAR é um método padrão e absolutamente seguro usado para testar o funcionamento do sistema antivírus. É seguro usá-lo, pois não se trata de um vírus real e não inclui fragmentos de código de vírus. A maioria dos produtos reage a este como se fosse um vírus (*embora sempre se refiram a ele com um nome óbvio, como "EICAR-AV-Test"*). É possível baixar o vírus EICAR no site www.eicar.com, onde você encontrará também todas as informações necessárias sobre o teste EICAR.

Tente baixar o arquivo ***eicar.com*** e salve-o em seu disco local. Logo após a confirmação do

download do arquivo de teste, a Proteção Online (*uma parte do componente Link Scanner*) reagirá a ele com um aviso. Esse aviso demonstra que o AVG está instalado corretamente em seu computador.



A partir do site http://www.eicar.com você também pode fazer o download da versão compactada do 'vírus' EICAR (*por exemplo, na forma de eicar_com.zip*). A Proteção Online permite que você baixe esse arquivo e salve-o no disco local, mas a Proteção Residente (*no componente Antivírus*) detecta o "vírus" enquanto você tenta descompactá-lo.

Se o AVG falhar na identificação do teste EICAR como sendo um vírus, você deverá verificar novamente a configuração do programa.

4.5. Configuração padrão do AVG

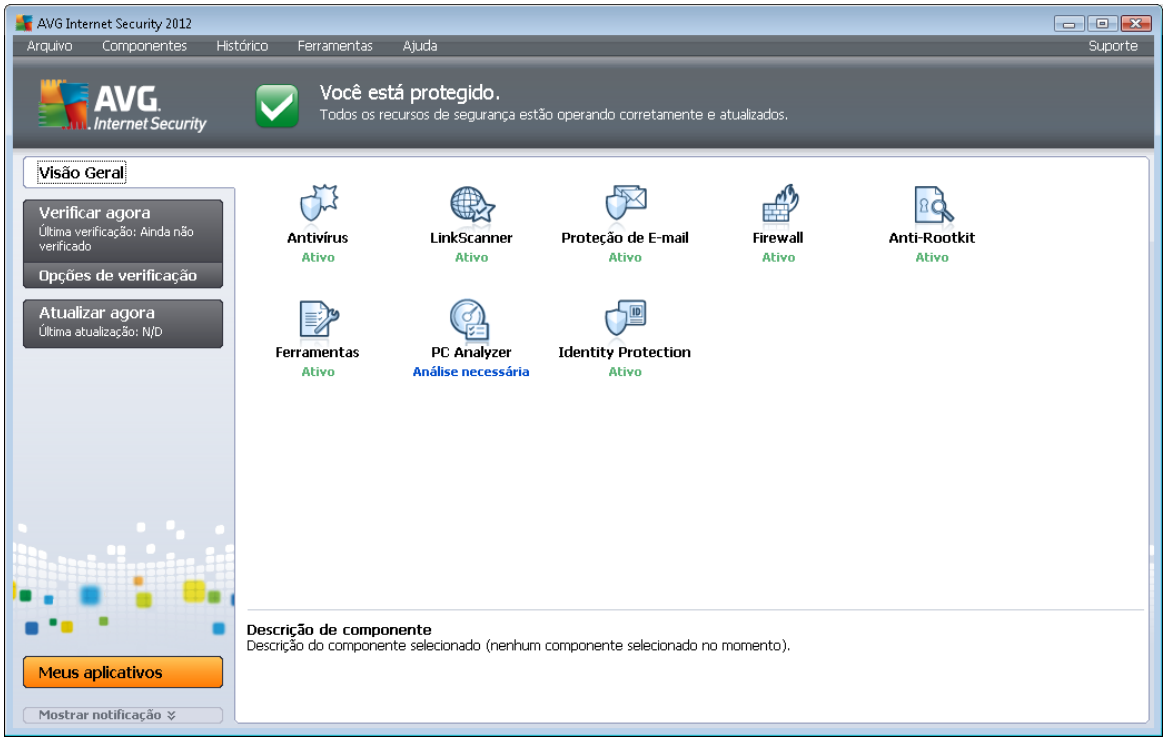
A configuração padrão (*isto é, como o aplicativo é configurado logo após a instalação*) de **AVG Internet Security 2012**é definida pelo fornecedor do software, de forma que todos os componentes e funções sejam ajustados para obter um desempenho ideal.

A menos que você tenha um motivo real para isso, não mude as configurações do AVG! Alterações nas configurações devem ser realizadas somente por um usuário experiente.

É possível acessar algumas edições menos importantes das configurações dos componentes do AVG diretamente na interface do usuário do componente específico. Se você tiver necessidade de alterar a configuração do AVG de acordo com suas necessidades, vá para Configurações Avançadas do AVG: selecione o item de menu do sistema ***Ferramentas/Configurações avançadas*** e edite a configuração do AVG na nova caixa de diálogo aberta, a Configurações avançadas do AVG.

5. Interface de usuário do AVG

O **AVG Internet Security 2012** é aberto com a janela principal:



A janela principal é dividida em várias seções:

- ***O Menu do Sistema*** *(linha do sistema superior na janela)* é a navegação padrão que permite acessar todos os componentes, serviços e recursos do **AVG Internet Security 2012** - detalhes >>
- ***Informações sobre o Status de Segurança*** *(seção superior da janela)* fornece informações sobre o status atual do **AVG Internet Security 2012** - detalhes >>
- ***Links Rápidos*** *(seção esquerda da janela)* permite acessar rapidamente as tarefas mais importantes e mais utilizadas do **AVG Internet Security 2012** - detalhes >>
- ***A seção Meus aplicativos*** *(seção inferior esquerda da janela)* abre uma visão geral de aplicativos adicionais disponíveis para o **AVG Internet Security 2012**: LiveKive, Family Safety e PC Tuneup
- ***Visão Geral dos Componentes*** *(seção central da janela)* oferece uma visão geral de todos os componentes instalados no **AVG Internet Security 2012** - detalhes >>
- ***Ícone na Bandeja do Sistema*** *(canto inferior direito do monitor, na bandeja do sistema)* indica o status atual do **AVG Internet Security 2012** detalhes >>
- ***Gadget AVG*** *(barra lateral do Windows, suportada no Windows Vista/7)* permite acesso rápido à atualização e à verificação no **AVG Internet Security 2012** - detalhes >>

5.1. Menu do sistema

O ***Menu do sistema*** é a navegação padrão usada em todos os aplicativos Windows. Está localizado horizontalmente, na parte superior da janela principal do AVG Internet Security 2012**.** Use o menu do sistema para acessar os componentes específicos do AVG, recursos e serviços.

O menu do sistema é dividido em cinco seções principais:

5.1.1. Arquivo

- ***Sair*** - fecha a interface do usuário do **AVG Internet Security 2012**. Entretanto, o aplicativo AVG continuará sendo executado em segundo plano e seu computador continuará protegido.

5.1.2. Componentes

O item Componentes do menu do sistema inclui links para todos os componentes do AVG instalados, abrindo sua caixa de diálogo padrão na interface do usuário:

- ***Visão geral do sistema*** - muda para a caixa de diálogo da interface padrão do usuário com a visão geral de todos os componentes instalados e seu status
- ***O componente Antivírus*** detecta vírus, spyware, worms, cavalos de Troia, arquivos executáveis indesejados ou bibliotecas em seu sistema, bem como protege você contra adwares maliciosos - detalhes >>
- ***O Link Scanner*** protege você contra ataques baseados na Web enquanto você faz pesquisas ou navega na Internet - detalhes >>
- ***A Proteção de E-mail*** verifica as mensagens de e-mail recebidas em busca de SPAM, além de bloquear vírus, ataques de phishing ou outras ameaças - detalhes >>
- ***O Firewall*** controla todas as comunicações em cada porta de rede, protegendo você contra ataques maliciosos e bloqueando todas as tentativas de intrusão - detalhes >>
- ***O Anti-Rootkit*** verifica rootkits perigosos ocultos em aplicativos, drivers ou bibliotecas - detalhes >>
- ***Ferramentas do Sistema*** oferece um resumo detalhado das informações do ambiente do AVG e do sistema operacional - detalhes >>
- ***O analisador PC Analyzer*** fornece informações sobre o status do seu computador - detalhes >>
- ***O Identity Protection*** protege constantemente seus ativos digitais contra novas e desconhecidas ameaças - detalhes >>
- ***Barra de Ferramenta de Segurança*** permite que você use funcionalidade selecionada do AVG diretamente do seu navegador Internet - >> detalhes
- ***Administração Remota*** exibida apenas no AVG Business Editions, caso você tenha

especificado durante o processo de instalação que esse componente deve ser instalado

5.1.3. Histórico

- Resultados da verificação - alterna para a interface de teste do AVG, especificamente para a caixa de diálogo Visão Geral dos Resultados da Verificação

- Detecção da Proteção Residente - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pela Proteção Residente

- Detecção do Verificador de e-mail - abre uma caixa de diálogo com uma visão geral dos anexos de e-mail detectados como perigosos pelo componente Verificador de E-mail

- Detecções da Proteção Online - abre uma caixa de diálogo com uma visão geral das ameaças detectadas pelo serviço Proteção Online no componente LinkScanner

- Quarentena de Vírus - abre a interface do espaço de quarentena (Quarentena de Vírus) no qual o AVG remove todas as infecções detectadas que, por algum motivo, não podem ser resolvidas automaticamente. No espaço de quarentena, os arquivos infectados são isolados e a segurança do computador é preservada, e, ao mesmo tempo, os arquivos infectados são armazenados para possível reparo futuro

- Log de histórico de eventos - abre a interface de log de histórico com uma visão geral de todas as ações registradas**AVG Internet Security 2012** .

- Firewall - abre a interface de configurações do firewall na guia Logs com uma visão geral detalhada de todas as ações do firewall

5.1.4. Ferramentas

- Verificar computador - alterna para a interface de verificação do AVG e inicia a verificação em todo o computador.

- Verificar pasta selecionada... - alterna para a interface de verificação do AVG e permite definir, na estrutura de árvore do computador, quais arquivos e pastas devem ser verificados.

- Verificar arquivo... - permite executar um teste sob demanda em um único arquivo selecionado na estrutura de árvore do disco.

- Atualizar - inicia automaticamente o processo de atualização **AVG Internet Security 2012** .

- ***Atualizar a partir do diretório...*** - executa o processo de atualização a partir dos arquivos de atualização localizados em uma pasta específica do disco local. Entretanto, esta opção é recomendada somente como emergência, ou seja, em situações em que não há conexão com a Internet (*por exemplo, seu computador está infectado e desconectado da Internet; seu computador está conectado a uma rede sem acesso à Internet, etc.*). Na nova janela aberta, selecione a pasta na qual colocou o arquivo de atualização anteriormente e inicialize o processo de atualização.

- Configurações avançadas... - abre a caixa de diálogo Configurações avançadas do AVG, na

qual é possível editar a configuração do AVG Internet Security 2012. Em geral, é recomendável manter as configurações padrão do aplicativo conforme definido pelo fornecedor do software.

- Configurações do Firewall... - abre uma caixa de diálogo independente para configuração avançada do componente Firewall.

5.1.5. Ajuda

- ***Conteúdo*** - abre os arquivos de ajuda do AVG
- ***Obter ajuda online*** - abre o site do AVG (http://www.avg.com/) na página de suporte técnico ao cliente
- ***Sua Web AVG*** - abre o site do AVG (http://www.avg.com/)
- ***Sobre vírus e ameaças*** - abre a Enciclopédia de vírus on-line, na qual é possível procurar informações sobre o vírus identificado
- ***Reativar*** - abre a caixa de diálogo ***Ativar AVG*** com os dados inseridos na caixa de diálogo Personalizar AVG do processo de instalação. Nessa caixa de diálogo é possível inserir o número da licença para substituir o número de vendas (*o número com o qual você instalou o AVG*) ou para substituir o número antigo da licença (*por exemplo, durante a atualização de um novo produto AVG*).
- ***Registre-se agora*** - estabelece uma conexão com a página de registro do site da AVG (http://www.avg.com/). Informe seus dados de registro. Somente os clientes que registrarem seus produtos AVG poderão receber suporte técnico gratuito.

Observação*: se estiver utilizando a versão de teste do* **AVG Internet Security 2012***, os dois últimos itens aparecerão como* ***Comprar agora*** *e* ***Ativar****, permitindo que você compre a versão completa do programa imediatamente. Para* **AVG Internet Security 2012** *instalado com um número de vendas, o itens são exibidos como****Registrar*** *e* ***Ativar****.*

- ***Sobre o AVG*** - abre a caixa de diálogo ***Informações*** com cinco guias que fornecem dados sobre o nome do programa, versão do programa e do banco de dados de vírus, informações do sistema, contrato de licença e informações de contato da ***AVG Technologies CZ***.

5.1.6. Suporte

O link ***Suporte*** abre uma nova caixa de diálogo de ***Informações*** com todos os tipos de informações de que você precisa para obter ajuda. A caixa de diálogo inclui dados básicos sobre o programa AVG instalado (*versão do banco de dados/programa*), detalhes da licença e uma lista de links de suporte rápido.

A caixa de diálogo ***Informações*** se divide em seis guias:fóruns

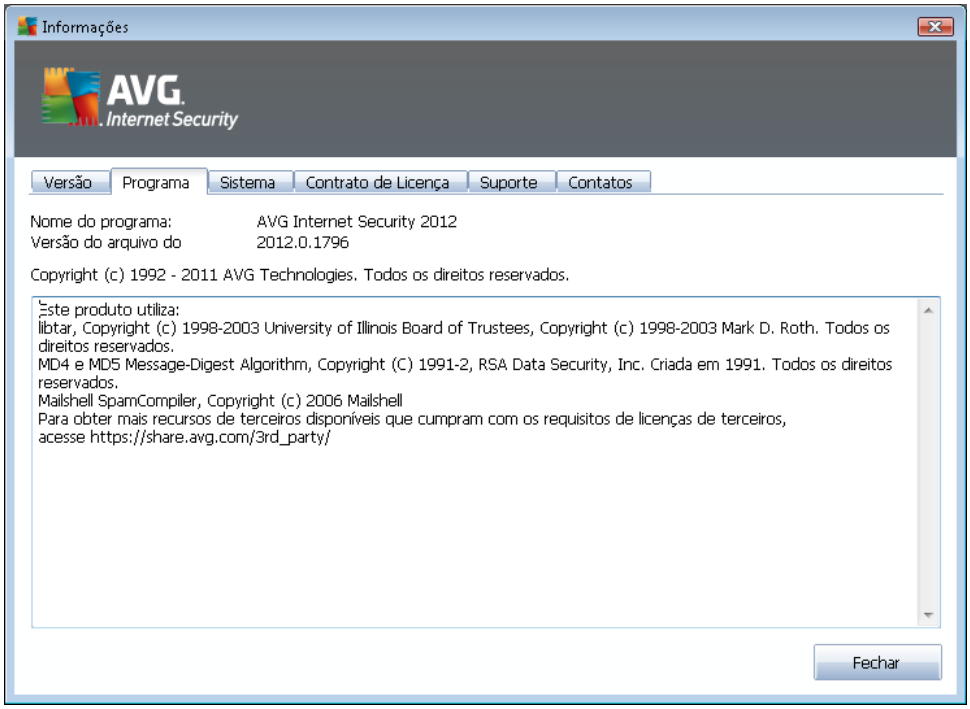
A guia ***Versão*** se divide em três seções:

- ***Informações de suporte*** - apresenta informações sobre a versão do **AVG Internet Security 2012**, a versão do banco de dados de vírus, a versão de banco de dados do Anti-Spam e a versão do LinkScanner.

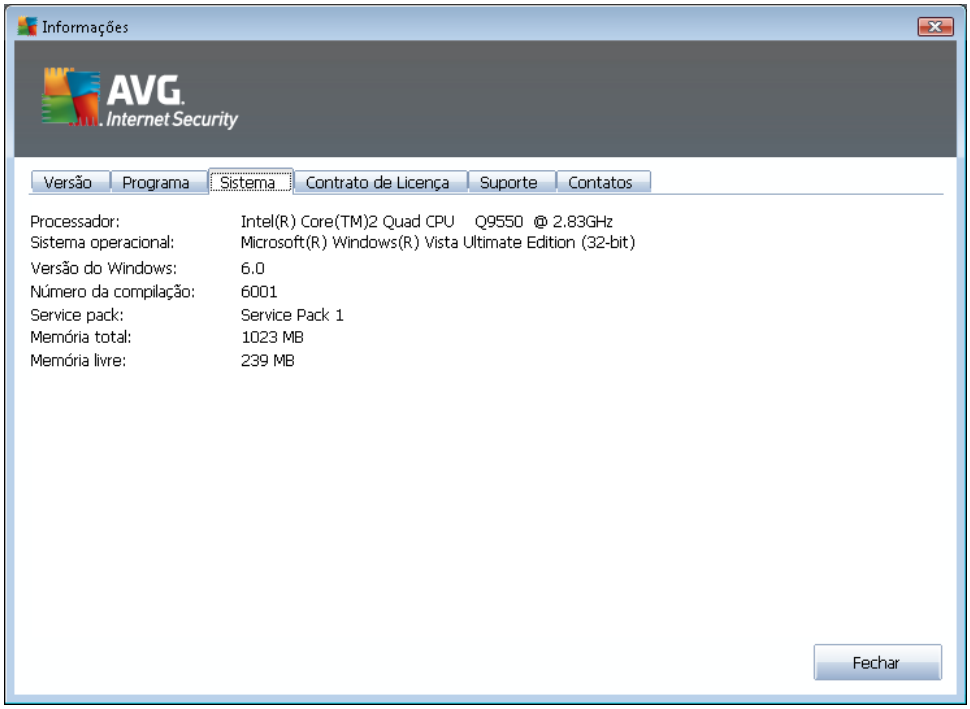
- ***Informações do usuário*** - apresenta informações sobre o usuário e a empresa licenciados.

- ***Detalhes da licença*** - apresenta informações sobre sua licença*(nome do produto, tipo de licença, número de licença, data de validade e número de computadores*). Nesta seção, você também pode usar o link ***Registro*** para registrar seu **AVG Internet Security 2012** online e desfrutar do Suporte técnico AVG completo. Além disso, é possível usar o link ***Reativar*** para abrir a caixa de diálogo ***Ativar o AVG***: insira seu número de licença no respectivo campo para substituir seu número de vendas *(que você usou durante a instalação do AVG Internet Security 2012)* ou para substituir seu número de licença atual *(por exemplo, para fazer o upgrade para um produto AVG mais completo).*

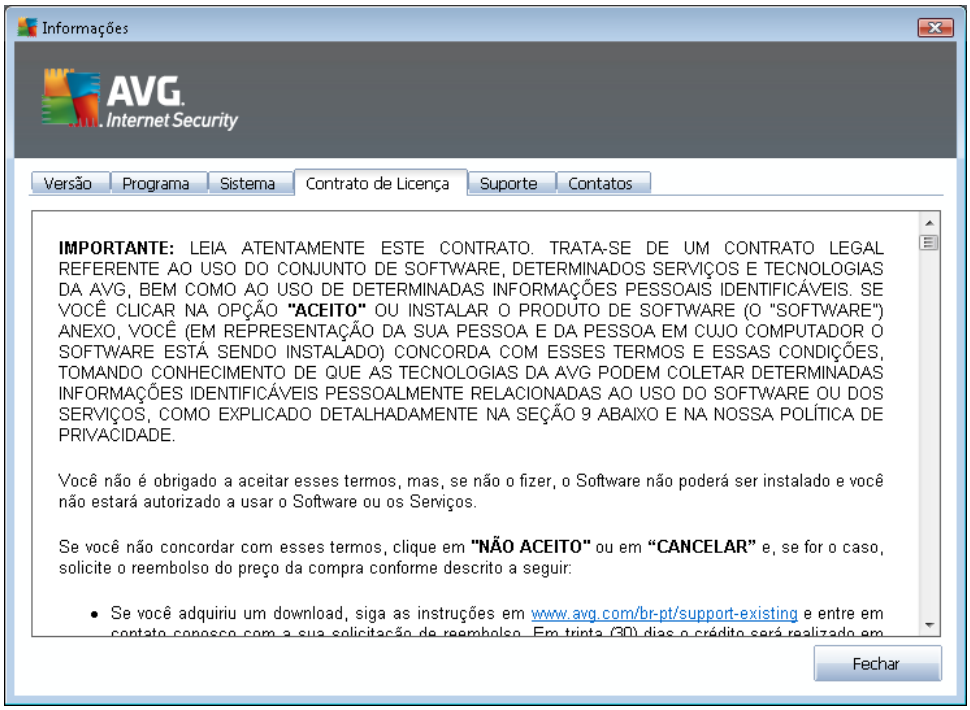
Na guia ***Programa*** , você pode encontrar informações sobre a versão de arquivo do programa **AVG Internet Security 2012** e sobre o código de terceiros usado no produto:



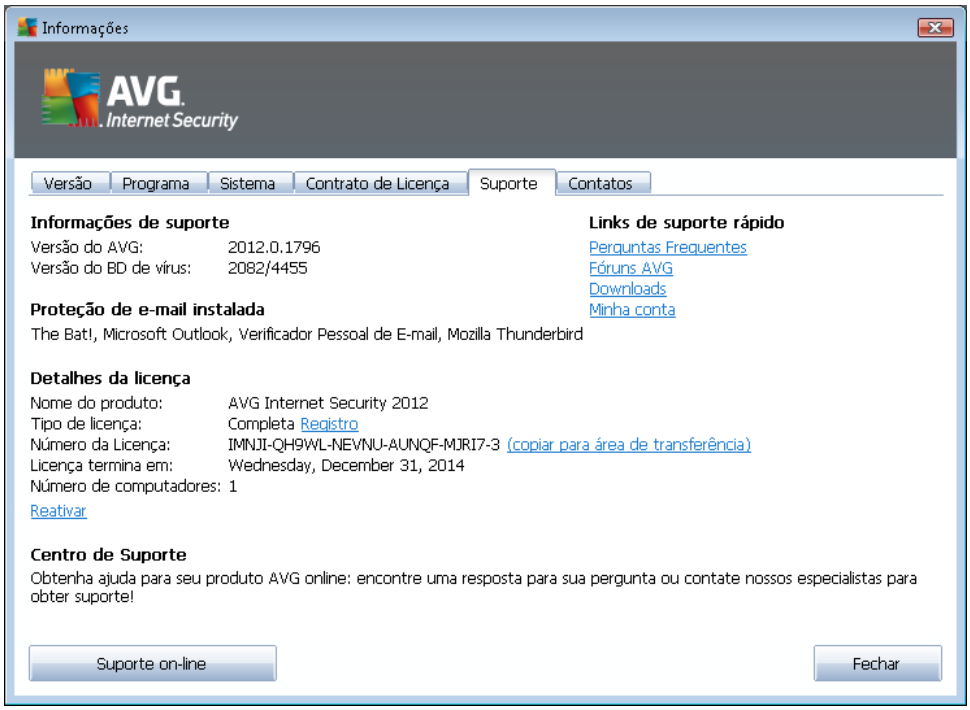
A guia ***Sistema*** oferece uma lista de parâmetros do seu sistema operacional *(tipo de processador, sistema operacional e versão, número da compilação, service packs usados, tamanho total da memória e espaço livre em disco)*:



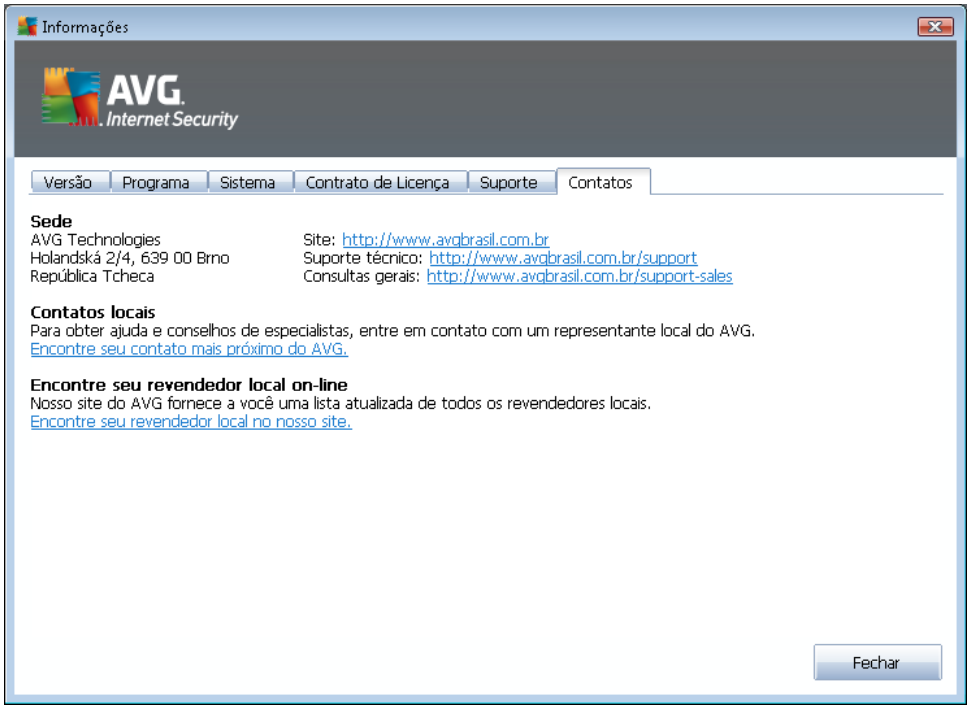
Na guia ***Contrato de licença***, você pode ler a versão completa do contrato de licença entre você e a AVG Technologies:



A guia ***Suporte*** apresenta uma lista de todas as possibilidade para você entrar em contato com o suporte ao cliente. Além disso, a guia apresenta links para o site do AVG (http://www.avg.com/), fóruns do AVG etc. Além disso, você pode encontrar informações que serão úteis durante o contato com a equipe de suporte ao cliente:



A guia ***Contatos*** fornece uma lista de todos os contatos da AVG Technologies e também dos contatos de revendedores e representantes locais da AVG:



5.2. Informações sobre status de segurança

A seção ***Informações sobre Status de Segurança*** está localizada na parte superior da janela principal do **AVG Internet Security 2012**. Nessa seção, você encontrará informações sobre o status de segurança atual do **AVG Internet Security 2012.** Observe uma visão geral dos ícones possivelmente ocultos dessa seção e seus significados:

- O ícone verde indica que o ***AVG Internet Security 2012 está totalmente funcional***. Seu computador está totalmente protegido, atualizado e todos os componentes instalados estão funcionando corretamente.

- O ícone laranja avisa que um ou mais componentes estão configurados incorretamente e você deverá prestar atenção às propriedades e configurações respectivas. Não há nenhum problema crítico no **AVG Internet Security 2012** e você provavelmente decidiu desativar alguns componentes por algum motivo. Você continua protegido! Entretanto, preste atenção às configurações do componente com problema! Seu nome será fornecido na seção ***Informações sobre*** o status de segurança.

O ícone alaranjado também aparecerá se, por algum motivo, você decidiu ignorar o status de erro de um componente. A opção ***Ignorar estado do componente*** está disponível no menu

contextual (*clique com o botão direito do mouse para abri-lo*) acima do ícone do respectivo componente na visão geral de componentes da janela principal do **AVG Internet Security 2012**. Selecione esta opção para informar que você está ciente do estado de erro do componente, mas que, por alguma razão, deseja continuar com o **AVG Internet Security 2012** e não quer ser avisado pelo ícone da bandeja do sistema. Talvez seja necessário usar esta opção em uma situação específica, mas é fortemente recomendável desativar a opção ***Ignorar estado do componente*** o mais rápido possível.

- O ícone vermelho indica que o ***AVG Internet Security 2012 se encontra em estado crítico***! Um ou mais componentes não estão funcionando corretamente e o **AVG Internet Security 2012** não poderá proteger seu computador. Preste atenção para reparar imediatamente o problema relatado. Se você não conseguir reparar o erro por conta própria, entre em contato com o Suporte técnico da AVG .

Caso o AVG Internet Security 2012 não tenha sido configurado para obter o melhor desempenho possível, um novo botão denominado Corrigir (ou Corrigir tudo, se o problema envolver mais de um componente) será exibido ao lado das informações sobre o status de segurança. Pressione o botão para iniciar um processo automático de Clique com o botão direito no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e configuração do programa. Essa é uma forma fácil de ajustar o AVG Internet Security 2012 para que ofereça o desempenho ideal e obtenha o nível de segurança máximo.

É altamente recomendável prestar atenção nas Informações sobre status de segurança e, caso o relatório indique algum problema, tentar resolvê-lo imediatamente. Caso contrário, seu computador estará sob risco!

Nota: *as informações sobre o status do AVG Internet Security 2012 também podem ser obtidas a qualquer momento no ícone da bandeja do sistema.*

5.3. Links rápidos

Os links rápidos estão localizados no lado esquerdo da interface de usuário do **AVG Internet Security 2012**. Esses links permitem que você tenha acesso imediato aos recursos do aplicativo mais importantes e mais usados, como a verificação e a atualização. Os links rápidos podem ser acessados em todas as caixas de diálogo da interface do usuário:

Os links rápidos são divididos graficamente em três seções:

- ***Visão geral*** - use este link para alternar de qualquer caixa de diálogo do AVG aberta no momento para a janela padrão com uma visão geral de todos os componentes instalados.. *(Para obter detalhes, consulte o capítulo Visão geral dos componentes)*

- ***Verificar agora*** - por padrão, este botão fornece informações sobre a última verificação executada *(por exemplo, o tipo de verificação e a data da execução mais recente)*. Clique no comando ***Verificar agora*** para iniciar a mesma verificação novamente. Se desejar executar outra verificação, clique no link ***Opções de verificação***. Com isso, você abrirá a interface de verificação do AVG, onde poderá executar e agendar verificações ou editar seus parâmetros. *(Para obter detalhes, consulte o capítulo Verificações do AVG)*

- ***Atualizar agora*** - este link informa a data e a hora em que a atualização mais recente foi realizada. Pressione o botão para executar o processo de atualização imediatamente e acompanhar o andamento. *(Para obter detalhes, consulte o capítulo Atualizações do AVG)*

Os links rápidos podem ser acessados na Interface de usuário do AVG a qualquer momento. Quando você usa um link rápido para executar um processo específico, seja uma verificação ou uma atualização, o aplicativo passa a exibir uma nova caixa de diálogo, mas os links rápidos permanecem disponíveis. Além disso, o processo em execução é apresentado graficamente com mais detalhes na navegação, para que você tenha controle total de todos os processos que estão sendo executados no **AVG Internet Security 2012** nesse momento.

5.4. Visão geral dos componentes

Seções Visão geral dos componentes

A seção ***Visão geral dos componentes*** se localiza na parte central da interface de usuário do **AVG Internet Security 2012**. A seção é dividida em duas partes:

- ***Visão geral de todos os componentes instalados***, que consiste em painéis gráficos de todos os componentes instalados. Cada painel é identificado pelo ícone do componente e fornece informações sobre se o componente respectivo está ativo ou inativo no momento.

- ***A descrição do componente*** está localizada na parte inferior da caixa de diálogo. A descrição oferece uma explicação breve sobre a funcionalidade básica do componente. Ela também fornece informações sobre o status atual do componente selecionado.

Lista dos componentes instalados

No **AVG Internet Security 2012** a seção***Visão geral dos componentes*** contém informações sobre os seguintes componentes:

- ***O componente Antivírus*** detecta vírus, spyware, worms, cavalos de Troia, arquivos executáveis indesejados ou bibliotecas em seu sistema, bem como protege você contra adwares maliciosos - detalhes >>

- ***O Link Scanner*** protege você contra ataques baseados na Web enquanto você faz pesquisas ou navega na Internet - detalhes >>

- ***A Proteção de E-mail*** verifica as mensagens de e-mail recebidas em busca de SPAM, além de bloquear vírus, ataques de phishing ou outras ameaças - detalhes >>
- ***O Firewall*** controla todas as comunicações em cada porta de rede, protegendo você contra ataques maliciosos e bloqueando todas as tentativas de intrusão - detalhes >>
- ***O Anti-Rootkit*** verifica rootkits perigosos ocultos em aplicativos, drivers ou bibliotecas - detalhes >>
- ***Ferramentas do Sistema*** oferece um resumo detalhado das informações do ambiente do AVG e do sistema operacional - detalhes >>
- ***O analisador PC Analyzer*** fornece informações sobre o status do seu computador - detalhes >>
- ***O Identity Protection*** protege constantemente seus ativos digitais contra novas e desconhecidas ameaças - detalhes >>
- ***Barra de Ferramenta de Segurança*** permite que você use funcionalidade selecionada do AVG diretamente do seu navegador Internet - detalhes >>

- ***Administração Remota*** exibida apenas no AVG Business Editions, caso você tenha especificado durante o processo de instalação que esse componente deve ser instalado

Ações acessíveis

- ***Mova o mouse sobre qualquer um dos ícones do componente*** para realçá-lo na visão geral dos componentes. Ao mesmo tempo, a descrição da funcionalidade básica do componente será exibida na parte inferior da interface do usuário.
- ***Clique uma vez em qualquer ícone do componente*** para abrir a interface dos componentes com uma lista de dados estatísticos básicos.
- ***Clique com o botão direito do mouse sobre um ícone do componente*** para expandir um menu contextual com várias opções:
  - ***Abrir*** - clique nesta opção para abrir a caixa de diálogo do próprio componente *(com um clique único no ícone do componente)*.
  - ***Ignorar o estado deste componente*** - selecione esta opção para expressar que está ciente do estado de erro do componente, mas, por algum motivo, você deseja manter este status e não quer receber avisos do ícone na bandeja do sistema.
  - ***Abrir em configurações avançadas ...*** - esta opção é disponível somente para alguns componentes, isto é, aqueles que oferecem configurações avançadas.

5.5. Ícone da bandeja do sistema

O ícone da bandeja do sistema do AVG *(na barra de tarefas do Windows, no canto inferior direito da tela)* indica o status atual do seu **AVG Internet Security 2012**. Ele está sempre visível na bandeja do sistema, estando a interface de usuário do seu **AVG Internet Security 2012** aberta ou fechada:

Exibição do ícone da bandeja do sistema do AVG

- Quando exibido em preto e branco, sem elementos adicionais, o ícone indica que todos os componentes do **AVG Internet Security 2012** estão ativos e totalmente funcionais. No entanto, o ícone também pode ser exibido dessa forma quando um dos componentes não está totalmente funcional, mas o usuário decidiu ignorar o estado do componente. *(Após ter confirmado a opção para ignorar o estado do componente, você está ciente do estado de erro do componente, mas, por algum motivo, deseja mantê-lo, por isso não deseja ser informado sobre a situação.)*

- O ícone com um ponto de exclamação indica que um *ou mais*componentes se encontram em estado de erro. Preste sempre atenção nesses avisos e tente remover o problema de configuração de um componente que não foi configurado corretamente. Para fazer alterações na configuração de um componente, clique duas vezes no ícone da bandeja do sistema para abrir a interface de usuário do aplicativo. Para obter informações detalhadas sobre os componentes que se encontram em estado de erro, consulte a seção de informações sobre o status de segurança.

- O ícone da bandeja do sistema também pode ser exibido em cores com um raio de luz que gira e pisca. Esta versão gráfica indica que há um processo de atualização em andamento.

- A exibição em cores com uma seta indica que há uma verificação do **AVG Internet Security 2012** em execução.

Informações do ícone da bandeja do sistema do AVG

O ícone da bandeja do sistema do AVG também mantém você informado sobre as atividades atuais do seu **AVG Internet Security 2012** e sobre possíveis alterações de status no programa(

como a execução automática de uma verificação ou atualização agendada, mudança de perfil do Firewall, alteração do status do componente, ocorrência de status de erro, ...) por uma janela pop-up aberta pelo ícone na bandeja do sistema:

Ações que podem ser acessadas no ícone da bandeja do sistema do AVG

O ícone da bandeja do sistema do AVG também pode ser usado como um link rápido para acessar a interface de usuário do **AVG Internet Security 2012**, clicando duas vezes no ícone. Ao clicar com o botão direito do mouse no ícone, você abre um menu de contexto breve com as opções a seguir:

- ***Abrir Interface de Usuário do AVG*** - clique para abrir a interface de usuário do **AVG Internet Security 2012**.
- ***Verificações*** - clique para abrir o menu de contexto das verificações predefinidas (*Verificar todo o computador*, *Verificar arquivos ou pastas específicos*, *Verificação Anti-Rootkit*) e selecione a verificação necessária. Ela será iniciada imediatamente.
- ***Firewall*** - clique para abrir o menu de contexto das opções de configurações de Firewall, onde é possível editar os principais parâmetros: status do Firewall (*Firewall ativado/Firewall desativado/modo Emergência*), mudança de modos de jogoe perfis de Firewall.
- ***Executar o PC Analyzer*** - clique para iniciar o componente PC Analyzer.
- ***Executando verificações*** - este item será exibido apenas se uma verificação estiver sendo executada no momento em seu computador. Para essa verificação, você pode definir sua prioridade ou, como segunda opção, interromper ou pausar a verificação em execução. Além disso, as seguintes ações estão acessíveis: *Definir prioridade para todas as verificações, Pausar todas as verificações* ou *Interromper todas as verificações*.
- ***Atualizar agora*** - inicia uma atualização imediata.
- ***Ajuda*** - abre o arquivo de ajuda da página de inicialização.

5.6. Gadget AVG

O gadget AVG é exibido na área de trabalho do Windows (*barra lateral do Windows*). Esse aplicativo tem suporte apenas nos sistemas operacionais Windows Vista e Windows 7. ***O gadget AVG*** oferece um acesso imediato às funções mais importantes do **AVG Internet Security 2012**, por exemplo, verificação e atualização:

Acesso rápido a verificação e atualização

Se necessário, o ***gadget AVG*** permite iniciar automaticamente uma verificação ou atualização:

- ***Verificar agora*** - clique no link ***Verificar agora*** para iniciar a verificação de todo o computador diretamente. Você pode acompanhar o progresso do processo de verificação na interface do usuário alternativa do gadget. Uma breve visão geral de estatísticas fornece informações sobre o número de objetos verificados, ameaças detectadas e ameaças reparadas. Durante a verificação, você pode sempre pausar ou interromper o processo de verificação. Para obter dados detalhados relacionados aos resultados da verificação, consulte a caixa de diálogo padrão Visão geral da verificação, que pode ser aberta diretamente no gadget, por meio da opção ***Mostrar detalhes*** *(os resultados da verificação serão listados na Barra lateral de verificação do gadget)*.

- ***Atualizar agora*** - clique no link ***Atualizar agora*****AVG Internet Security 2012** para iniciar a atualização do diretamente do gadget:

Acesso a redes sociais

O Gadget AVG também oferece conexões de link rápido às principais redes sociais. Use o botão

respectivo para conectar-se a comunidades do AVG no Twitter, Facebook ou LinkedIn:

- ***Link no Twitter*** - abre uma nova interface do ***gadget AVG***, fornecendo uma visão geral dos feeds mais recentes da AVG postados no Twitter. Siga o link ***Ver todos os feeds da AVG no Twitter*** para abrir o navegador em uma nova janela, e você será redirecionado diretamente ao site do Twitter, especificamente à página dedicada às notícias relacionadas à AVG:

- ***Link do Facebook*** - abre o navegador no site do Facebook, especificamente na página da ***Comunidade da AVG***

- ***LinkedIn*** - esta opção só está disponível na instalação de rede (*ou seja, desde que você tenha instalado o AVG usando uma das licenças do AVG Business Editions*), e ele abre o seu navegador de internet no site ***Comunidade AVG SMB*** dentro da rede social LinkedIn

Outros recursos acessados via gadget

- ***PC Analyzer*** - abre a interface do usuário no componente PC Analyzer

- ***Caixa Procurar*** - digite uma palavra-chave e obtenha os resultados da pesquisa imediatamente em uma nova janela aberta com o seu navegador padrão

6. Componentes do AVG

6.1. Antivírus

O componente ***Antivírus*** é a base do **AVG Internet Security 2012** e combina diversos recursos fundamentais de um programa de segurança:

- Mecanismo de verificação
- Proteção Residente
- Proteção Anti-spyware

6.1.1. Mecanismo de verificação

O mecanismo de verificação, que é a base do componente ***Antivírus***, verifica todos os arquivos e a atividade dos mesmos *(arquivos que são abertos e fechados etc.)*. Todos os vírus detectados serão bloqueados e não poderão realizar nenhuma ação. Eles também serão limpos e colocados na Quarentena de Vírus.

A principal característica da proteção do AVG Internet Security 2012 é que nenhum vírus conhecido pode ser executado no computador!

Métodos de detecção

A maioria dos softwares antivírus usa a verificação heurística, em que os arquivos são verificados no que diz respeito às características normais de vírus, as chamadas assinaturas virais. Isso significa que o verificador antivírus pode detectar um vírus novo e desconhecido se este contiver algumas características típicas dos vírus existentes. ***O Antivírus*** usa os seguintes métodos de detecção:

- Verificação - procura seqüências de caracteres típicas de um determinado vírus.
- *Análise heurística* - emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual
- Detecção genérica - detecção de instruções características de um determinado vírus ou grupo de vírus

Nas situações em que uma única tecnologia poderia falhar na detecção ou identificação de um vírus, o ***Antivírus*** combina várias tecnologias para assegurar que o computador fique protegido. O **AVG Internet Security 2012** também é capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL que possam ser potencialmente indesejáveis no sistema. Chamamos essas ameaças de Programas Potencialmente Indesejáveis *(vários tipos de spyware, adware etc.)*.. Além disso, o **AVG Internet Security 2012** verifica o registro do sistema à procura de entradas suspeitas, arquivos temporários da Internet e cookies de rastreamento, bem como permite tratar todos os itens potencialmente perigosos da mesma maneira que qualquer outra infecção.

O AVG Internet Security 2012 oferece proteção ininterrupta para seu computador!

6.1.2. Proteção Residente

O* AVG Internet Security 2012** oferece proteção contínua na forma da proteção residente. ***O componente Antivírus verifica cada arquivo *(de extensões específicas ou de qualquer extensão)* que é aberto, salvo ou copiado. Ele protege as áreas do sistema do computador e mídias removíveis (*disco flash etc.*). Se um vírus é detectado em um arquivo acessado, a proteção residente interrompe a operação em execução no momento e não permite que o vírus seja ativado. Normalmente, você nem se dará conta do processo, já que a proteção residente será executada "em segundo plano". Você somente é notificado quando as ameaças são encontradas, ao mesmo tempo que o ***Antivírus*** bloqueia a ativação da ameaça e a remove.

A proteção residente é carregada na memória do computador durante a inicialização, e é vital que você a mantenha sempre ativada.

6.1.3. Proteção Anti-spyware

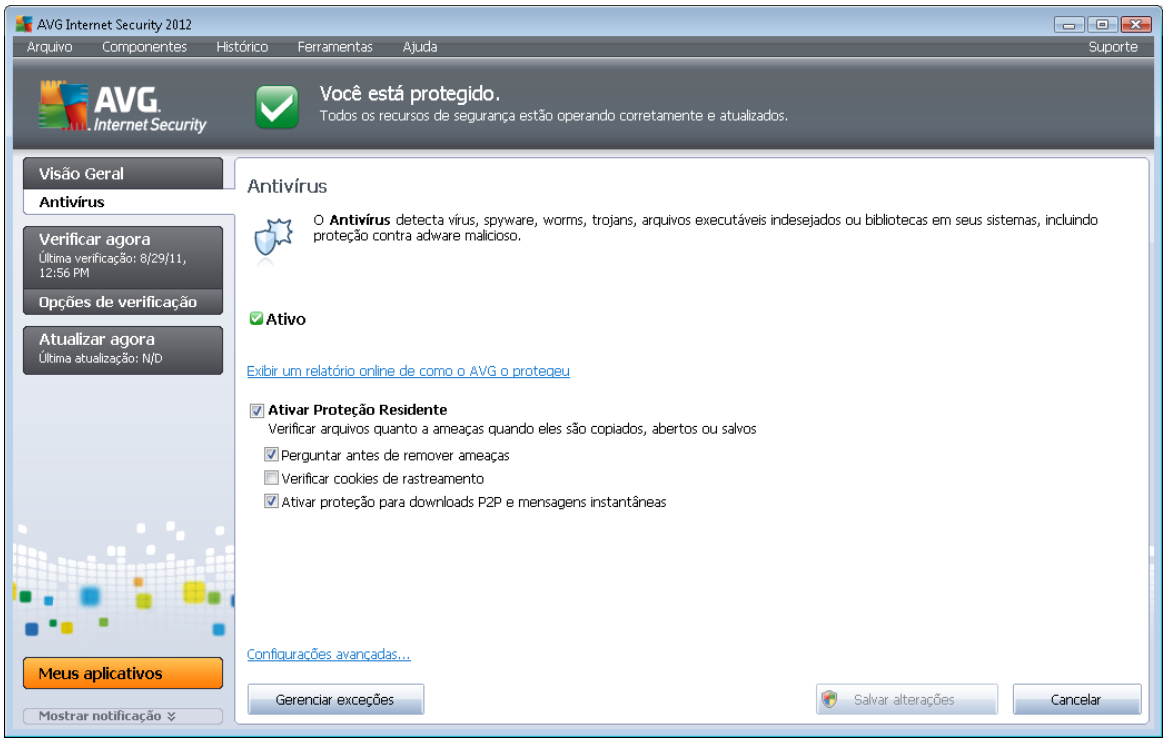
O recurso ***Anti-Spyware*** consiste em um banco de dados de spyware usado para identificar tipos conhecidos de definições de spyware. Os especialistas em spyware da AVG trabalham continuamente para identificar e descrever os mais recentes padrões de spyware assim que surgem, além de adicionar as definições ao banco de dados. Através do processo de atualização, essas novas definições são baixadas para o seu computador, para que fique sempre protegido, até mesmo dos mais novos tipos de spyware. ***O Anti-Spyware*** permite que você faça uma verificação completa no computador em busca de malware/spyware. Ele também detecta malwares inativos e não perigosos, ou seja, baixados mas ainda não ativados.

O que é um spyware?

Normalmente, o spyware é definido como um tipo de malware, ou seja, software que coleta informações a partir do computador do usuário sem o conhecimento ou consentimento dele. Alguns aplicativos de spyware também podem ser instalados propositalmente e, em geral, contêm anúncios, janelas pop-up ou tipos diferentes de softwares inoportunos. Atualmente, a fonte mais comum de infecção são sites com conteúdo potencialmente perigoso. Outros métodos de transmissão, como e-mail ou worms e vírus, são também predominantes. A proteção mais importante é o uso de um verificador de segundo plano sempre ativo, o ***Anti-Spyware***, que funciona como uma proteção residente e verifica seus aplicativos em segundo plano, à medida que são executados.

6.1.4. Interface do Antivírus

A interface do componente ***Antivírus*** fornece informações resumidas sobre a funcionalidade, sobre o status *(Ativo)* e opções de configuração básica do componente:



Opções de configuração

A caixa de diálogo fornece opções de configuração básicas dos recursos disponíveis no componente ***Antivírus***. A seguir, você pode encontrar uma breve descrição dessas opções:

- ***Exibir um relatório online de como o AVG o protegeu*** - o link redireciona você a uma página específica no site do AVG (http://www.avg.com/). Na página, é possível encontrar um resumo estatístico detalhado de todas as atividades realizadas pelo **AVG Internet Security 2012** em seu computador em um período específico e ao todo.

- ***Proteção Residente*** - esta opção permite ativar/desativar facilmente a proteção residente. A Proteção Residente verifica os arquivos à medida que são copiados, abertos ou salvos. Quando um vírus ou qualquer tipo de ameaça for detectado, você será alertado imediatamente. Por padrão, a função é ativada e recomenda-se que permaneça com essa configuração. Com a proteção residente, é possível decidir como as infecções possivelmente detectadas devem ser tratadas:

    - ***Remover todas as ameaças automaticamente*/*Perguntar antes de remover ameaças*** - selecione uma dessas opções. Esta opção não afeta o nível de segurança e se reflete apenas em suas preferências.

- ***Verificar cookies de rastreamento*** - independentemente das opções anteriores, você pode decidir se deseja verificar os cookies de rastreamento. *(Os cookies são parcelas de texto enviadas por um servidor a um navegador da Web e devolvidas inalteradas pelo navegador sempre que ele acessa esse servidor. Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas.)* Em casos específicos, você pode ativar esta opção para obter níveis de segurança máximos, mas ela fica desativada por padrão.

- ***Ativar proteção de Mensagens Instantâneas*** - marque este item se deseja confirmar se a comunicação por mensagens instantâneas (*como ICQ, MSN Messenger...*) está livre de vírus.

- ***Configurações avançadas***... - clique no link para ser redirecionado para a caixa de diálogo Configurações avançadas do **AVG Internet Security 2012**. Lá você pode editar a configuração dos componentes em detalhes. Contudo, observe que a configuração padrão de todos os componentes é definida de modo que o **AVG Internet Security 2012** proporcione o melhor desempenho e segurança máxima. A menos que você tenha um motivo real para fazê-lo, recomenda-se manter a configuração padrão.

Botões de controle

Na caixa de diálogo, você pode usar os seguintes botões de controle:

- ***Gerenciar exceções*** - abra uma nova caixa de diálogo intitulada Proteção Residente - Exceções. A caixa de diálogo também pode ser acessada pelo menu principal, seguindo esta sequência Configurações avançadas/Antivírus/Proteção Residente/Exceções *(consulte o capítulo correspondente para obter descrições detalhadas)*. Na caixa de diálogo, você pode especificar arquivos e pastas que devem ser excluídos da verificação da Proteção Residente. Se isso não for necessário, é altamente recomendável não excluir nenhum item. Essa caixa de diálogo fornece os seguintes botões de controle:

  - *Adicionar Caminho* – especifique um diretório *ou diretórios* a serem excluídos da verificação, selecionando-os individualmente na árvore de navegação do disco local.

  - *Adicionar Arquivo* – especifique arquivos a serem excluídos da verificação, selecionando-os um a um na árvore de navegação do disco local.

  - *Editar Item* – permite editar o caminho especificado para um arquivo ou pasta selecionado.

  - *Remover Item* – permite excluir o caminho para um item selecionado da lista.

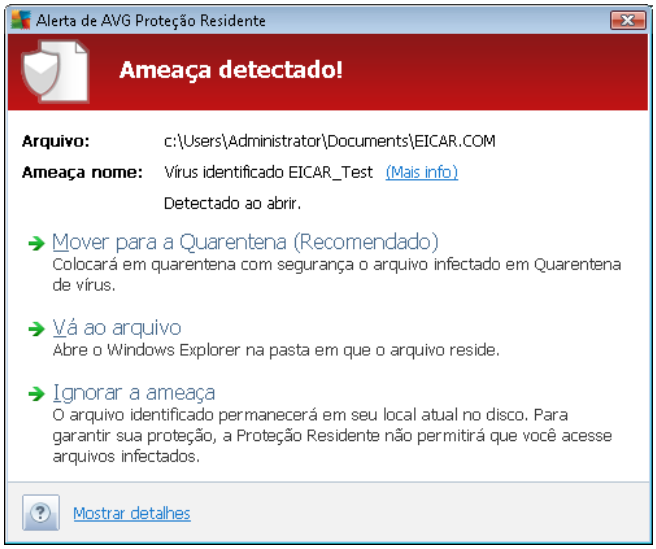
- ***Salvar alterações*** - salve todas as alterações nas configurações do componente realizadas nesta caixa de diálogo e volte à interface de usuário principal do **AVG Internet Security 2012** (*visão geral dos componentes*).

- ***Cancelar*** - cancele todas as alterações realizadas nas configurações do componente desta caixa. Nenhuma alteração será salva. Você voltará à interface de usuário principal do **AVG Internet Security 2012** (*visão geral dos componentes*).

6.1.5. Detecções de Proteção Residente

Ameaça detectada!

A Proteção Residente verifica os arquivos à medida que são copiados, abertos ou salvos. Quando um vírus ou qualquer tipo de ameaça é detectado, você é alertado imediatamente por meio da seguinte caixa de diálogo:



Nessa caixa de diálogo de aviso, você encontrará dados sobre o arquivo detectado e considerado infectado (*Nome do arquivo*), o nome da infecção reconhecida (*Nome da ameaça*) e um link para a Enciclopédia de vírus, na qual você pode encontrar informações detalhadas sobre a infecção detectada, se conhecida (*Mais informações*).

Além disso, você deve decidir a ação a ser executada agora. Há várias opções disponíveis. ***Observe que, em condições específicas (o tipo de arquivo infectado e sua localização), nem todas as opções estarão sempre disponíveis!***

- ***Remover ameaça como Usuário avançado*** – marque a caixa se supor que pode não ter direitos suficientes para remover a ameaça como um usuário comum. Usuários avançados possuem direitos de acesso amplos e se a ameaça estiver localizada em uma certa pasta do sistema, você pode precisar usar essa caixa de seleção para removê-la com sucesso.

- ***Reparar*** - este botão será exibido apenas se a infecção detectada puder ser reparada. Em seguida, ela é removida do arquivo e restaura o estado original do arquivo. Se o próprio arquivo for um vírus, use esta função para excluí-lo (*por exemplo, removido para a Quarentena*)

- ***Mover para Quarentena*** - o vírus será movido para a Quarentena de vírus do

- ***Ir para o arquivo*** - essa opção redireciona o usuário ao local exato do objeto suspeito (*abre a nova janela do Windows Explorer*)

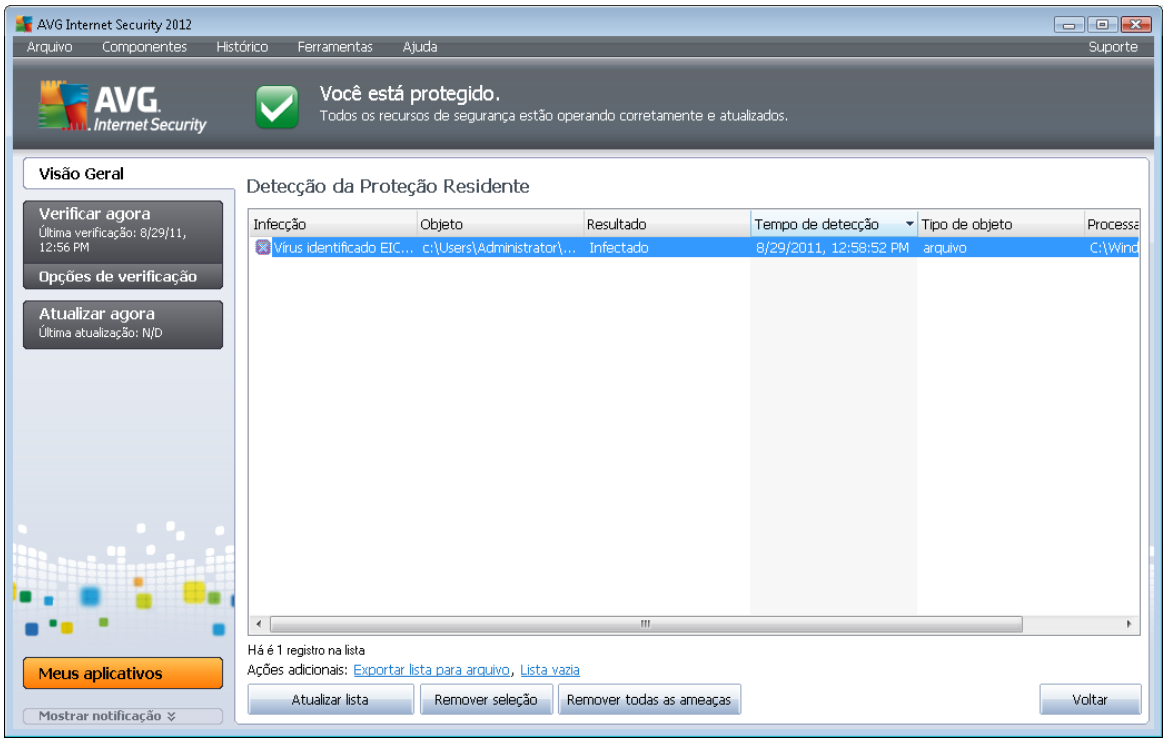
- ***Ignorar*** - NÃO recomendamos o uso desta opção, a não ser que exista um bom motivo!

Nota: *Pode acontecer do tamanho do objeto detectado exceder o limite de espaço livre na Quarentena de Vírus. Nesse caso, uma mensagem de aviso será exibida informando sobre o problema enquanto você tenta mover o objeto infectado para a Quarentena de Vírus. No entanto, o tamanho da Quarentena de Vírus pode ser editado. Ele é definido como uma porcentagem ajustável do tamanho real do disco rígido. Para aumentar o tamanho da Quarentena de Vírus, vá para a caixa de diálogo Quarentena de vírus dentro de Configurações avançadas do AVG, na opção "Limitar o tamanho da Quarentena de Vírus".*

Na seção inferior da caixa de diálogo, você encontrará o link ***Mostrar detalhes*** - clique nele para abrir uma janela popup com informações detalhadas sobre o processo em execução enquanto a infecção foi detectada e a identificação do processo.

Visão geral das detecções da Proteção Residente

A visão geral completa de todas as ameaças detectadas pela Proteção Residente está disponível na caixa de diálogo ***Detecção da Proteção Residente***, acessível por meio da opção de menu do sistema Histórico/detecção da Proteção Residente:



A ***detecção da Proteção Residente*** oferece uma visão geral dos objetos detectados pela Proteção Residente, avaliados como perigosos e recuperados ou movidos para a Quarentena de vírus. Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção*** - descrição (possivelmente até o nome) do objeto detectado

- ***Objeto*** - localização do objeto
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que o objeto foi detectado
- ***Tipo de Objeto*** - tipo de objeto detectado
- ***Processo*** - qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir todas as entradas de objetos detectados (***Lista vazia***). O botão ***Atualizar lista*** atualizará a lista de detecções feitas pela ***Proteção Residente*** . O botão ***Voltar*** leva você de volta à interface de usuário inicial padrão do AVG (*visão geral dos componentes*).

6.2. Link Scanner

O LinkScanner protege contra o crescente número de ameaças atuais e que estão surgindo na Web. Essas ameaças podem estar escondidas em qualquer tipo de site, de governamentais a grandes marcas bem conhecidas, a pequenas empresas, e raramente permanecem nesses locais mais de 24 horas. ***O LinkScanner*** protege analisando as páginas da web que estão por trás de todos os links em qualquer página da Web que esteja vendo e garantindo que são seguras só no momento que importa – quando você está prestes a clicar nesse link.

O LinkScanner não se destina à proteção de plataformas de servidores.

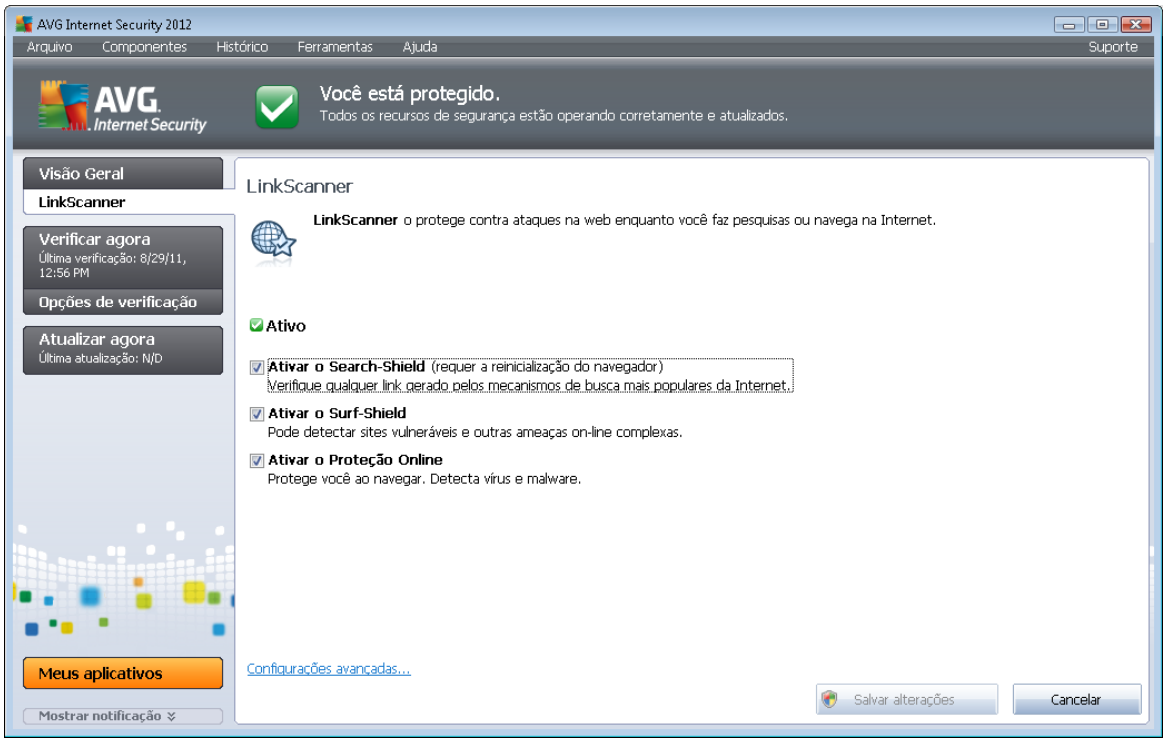
A tecnologia ***LinkScanner*** consiste nos seguintes recursos principais:

- O Search-Shield contém a lista de sites ((endereços de URL) que são conhecidos por serem perigosos. Em pesquisas no Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask e Seznam, todos os resultados da pesquisa são verificados de acordo com essa lista, e é mostrado um ícone de veredito *(para Yahoo! apenas ícones de veredictos "site explorado" são mostrados)*.
- O Surf-Shield verifica o conteúdo dos sites que você estiver visitando, independente do endereço deles. Mesmo se algum site não for detectado pelo Search-Shield *(por exemplo, quando um novo site mal-intencionado é criado, ou quando um site anteriormente limpo agora contém algum malware*), ele será detectado e bloqueado pelo Surf-Shield quando você tentar visitá-lo.
- A Proteção Online funciona como uma proteção em tempo real enquanto você navega pela Internet. Esse recurso verifica o conteúdo de páginas da Web visitadas e os possíveis arquivos incluídos nelas, mesmo antes de elas serem exibidas no navegador da Web ou baixadas no computador. A Proteção Online detecta vírus e spyware contidos na página que você vai visitar e interrompe o download instantaneamente para que nenhuma ameaça chegue até seu computador.
- ***O AVG Accelerator*** permite uma reprodução melhor de vídeos online e facilita downloads

adicionais. Quando o processo de aceleração de vídeo estiver em andamento, você não será notificado pela janela de pop-up na bandeja do sistema.

6.2.1. Interface do Link Scanner

A caixa de diálogo principal do componente LinkScanner fornece uma breve descrição da funcionalidade do componente, bem como informações sobre seu status atual *(Ativo)*:



Na parte inferior da caixa de diálogo, algumas configurações básicas dos componentes estão disponíveis:

- ***Ativar Search-Shield*** - (*ativado por padrão*): desmarque a caixa somente se tiver um bom motivo para desativar a funcionalidade Search Shield.
- ***Ativar Surf-Shield*** - (*ativado por padrão*): proteção ativa (*em tempo real*) contra sites exploradores, à medida que são acessados. As conexões conhecidas com sites maliciosos e seu conteúdo exploratório são bloqueadas à medida que são acessados por meio de um navegador da Web *ou outro aplicativo que utilize HTTP*).
- ***Ativar Proteção Online*** - (*ativado por padrão*): verificação de vírus e spyware em tempo real nas páginas da Web que você está prestes a visitar. Se algo for detectado, o download será interrompido imediatamente, para que nenhuma ameaça atinja seu computador.

6.2.2. Detecções do Search-Shield

Ao pesquisar na Internet com o ***Search-Shield***ativado, todos os resultados retornam dos mecanismos de busca mais conhecidos, como*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, and SlashDot*) são analisados com relação a links perigosos ou suspeitos. Ao verificar esses links e marcar os perigosos, o Link Scanner indicará o problema antes de você clicar em links suspeitos ou perigosos, portanto você poderá ter certeza de que acessará apenas sites seguros.

Quando um link estiver sendo avaliado na página de resultados da pesquisa, você verá um sinal gráfico próximo ao link informando que a verificação do link está em andamento. Quando a avaliação estiver terminada, o respectivo ícone informativo será exibido:

A página do link é segura (*este ícone não será exibido para resultados de pesquisa seguros resultados de pesquisa JP*).

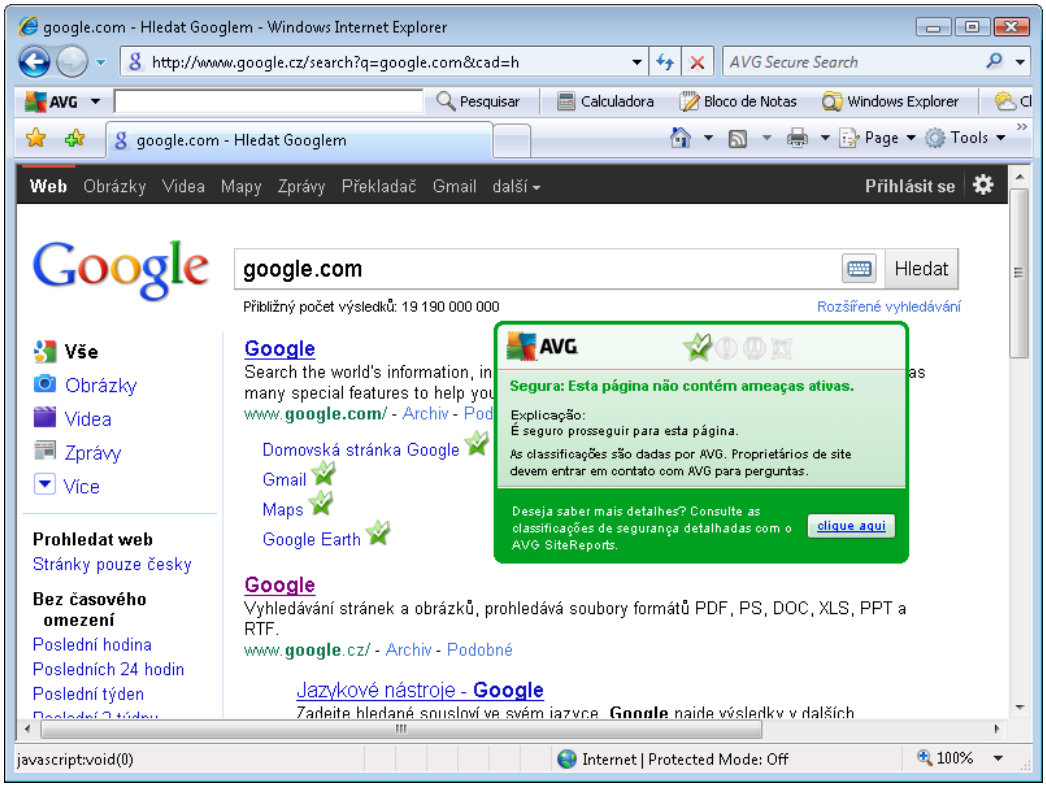
A página do link não contém ameaças, mas é suspeita (*de origem ou intenção duvidosa, portanto, não é recomendada para compras online etc.*).

A página de link pode ser segura, mas contém outros links para páginas definitivamente perigosas, ou de código suspeito, embora não esteja diretamente empregando uma ameaça no momento.

A página de link contém ameaças ativas! Para sua própria segurança, você não poderá visitar esta página.

A página do link não está acessível e não pôde ser verificada.

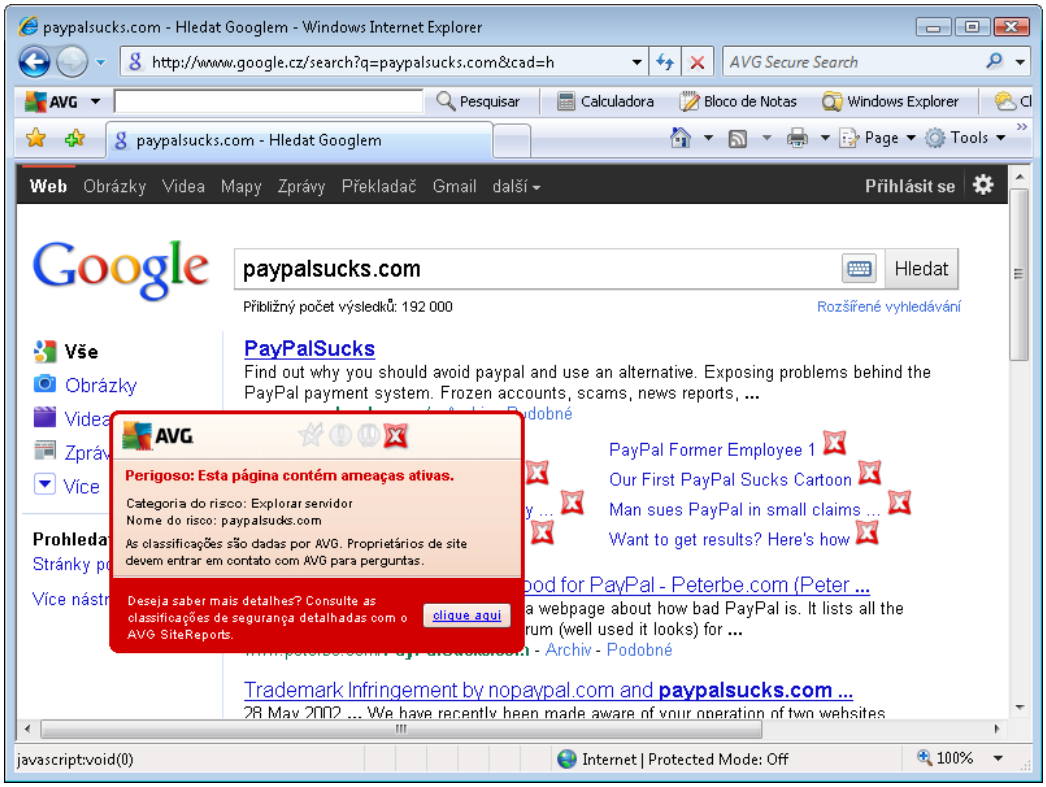
Passar o mouse sobre um ícone de classificação individual exibirá detalhes sobre o link específico em questão. As informações incluem detalhes adicionais da ameaça (*se existir alguma*):



6.2.3. Detecções do Surf-Shield

Essa poderosa proteção bloqueará o conteúdo mal-intencionado de qualquer página da Web que você tente abrir e impedirá que seja baixada para o seu computador. Com esse recurso ativado, clicar em um link ou digitar uma URL para um site perigoso bloqueará automaticamente a abertura da página da Web, protegendo-o inadvertidamente contra infecção. É importante lembrar que as páginas da Web exploradas podem infectar seu computador simplesmente com uma visita ao site afetado; por isso, quando você solicitar uma página da Web perigosa contendo explorações ou outras ameaças sérias, o Link Scanner não permitirá que seu navegador a exiba.

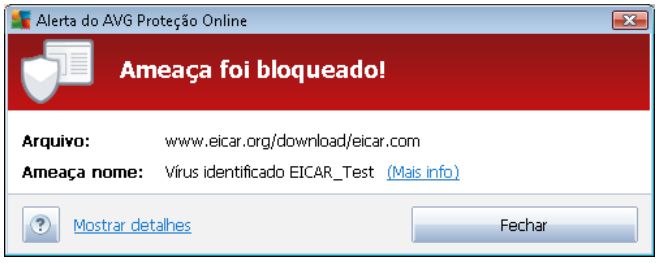
Se você encontrar um site malicioso em seu navegador da Web, o LinkScanner emitirá um aviso com uma tela semelhante a esta:



A inserção de um site da Web como este é altamente de risco e, portanto, não é recomendada!

6.2.4. Detecções da Proteção Online

A Proteção Online verifica o conteúdo de páginas da Web visitadas e possíveis arquivos incluídos nelas mesmo antes de elas serem exibidas no navegador da Web ou baixadas para o seu computador. Se uma ameaça for detectada, você será alertado imediatamente pela seguinte caixa de diálogo:



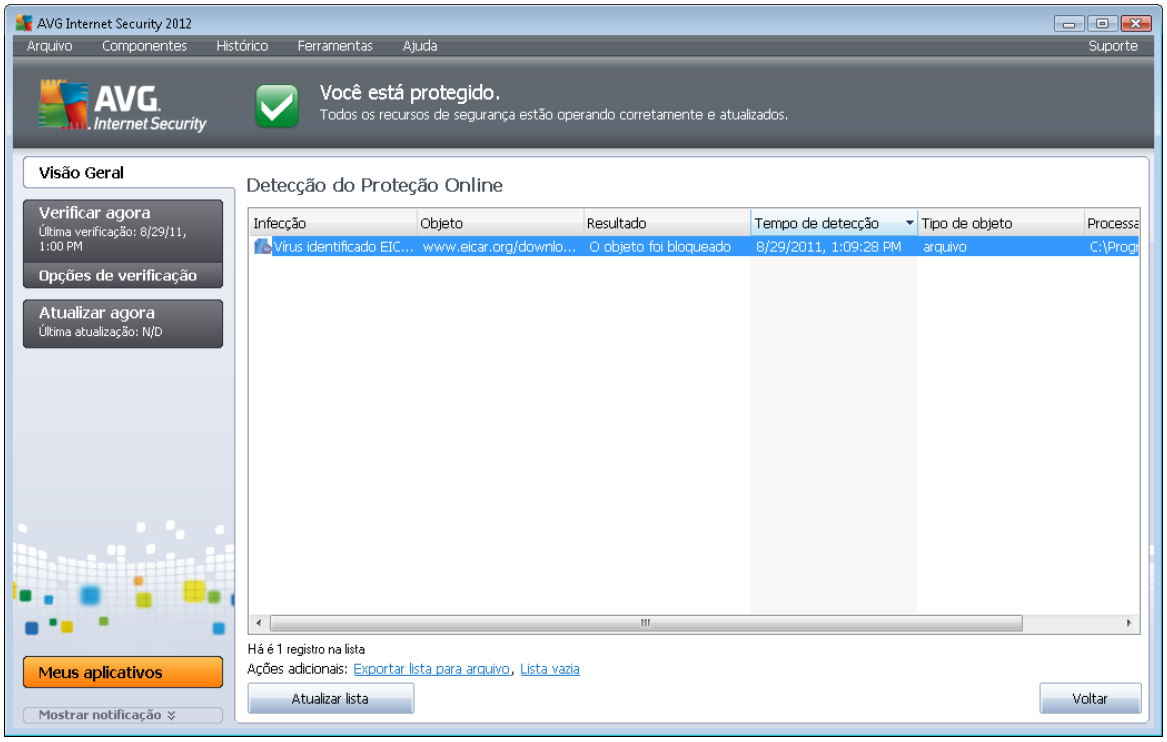
Nessa caixa de diálogo de aviso, você encontrará dados sobre o arquivo detectado e considerado infectado (*Nome do arquivo*), o nome da infecção reconhecida (*Nome da ameaça*) e um link para a Enciclopédia de vírus, na qual você pode encontrar informações detalhadas sobre a infecção detectada (*se conhecida*). Essa caixa de diálogo fornece os seguintes botões:

- ***Mostrar detalhes*** - clique no botão ***Mostrar detalhes*** para abrir uma nova janela popup, na qual você pode encontrar informações sobre o processo em execução enquanto a infecção

foi detectada e a identificação do processo.

- ***Fechar*** - clique no botão para fechar a caixa de diálogo de aviso.

A página da Web suspeita não será aberta, e a detecção da ameaça será registrada na lista de ***Detecções da Proteção Online*** - essa visão geral de ameaças detectadas está acessível no menu do sistema Histórico/detecções da Proteção Online.



Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção***- descrição (*possivelmente até o nome*) do objeto detectado
- ***Objeto*** - origem do objeto (*página da Web*)
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que a ameaça foi detectada e bloqueada
- ***Tipo de Objeto*** - tipo de objeto detectado
- ***Processo*** - qual ação foi executada para ativar o objeto potencialmente perigoso de modo a permitir que fosse detectado

Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir todas as entradas de objetos detectados (***Lista vazia***).

Botões de controle

- ***Atualizar lista*** - atualiza a lista de detecções feitas pela ***Proteção Online***
- ***Voltar*** - volta para a caixa de diálogo principal padrão do AVG *(visão geral dos componentes).*

6.3. Proteção de E-mail

O e-mail é uma das fontes mais comuns de vírus e cavalos de tróia. O phishing e o spam tornam o e-mail uma fonte de riscos ainda maior. Contas gratuitas de e-mail são as que têm maior probabilidade de receber mensagens de e-mail mal-intencionadas (*já que raramente adotam tecnologias anti-spam*), e os usuários domésticos confiam demais nesse tipo de conta de e-mail. Além dos usuários domésticos, sites desconhecidos e formulários de preenchimento on-line com dados pessoais (*como endereço de e-mail*) aumentam a exposição a ataques via e-mail. Em geral, as empresas usam contas de e-mail corporativo e adotam filtros anti-spam, etc., para reduzir o risco.

O componente ***Proteção de E-mail*** é responsável por verificar cada mensagem de e-mail, enviada ou recebida. Quando um vírus é detectado em um e-mail, ele é removido para a Quarentena de vírus imediatamente. O componente também pode filtrar determinados tipos de anexos de e-mail e adicionar um texto de certificação a mensagens sem infecção. ***A Proteção de E-mail*** consiste em duas funções principais:

- Verificador de E-mail
- Antispam

6.3.1. Verificador de E-mail

Verificador Pessoal de E-mail verifica e-mails de entrada/saída automaticamente. É possível usá-lo com clientes de email que não têm seu próprio plugin no AVG (*mas pode também ser usado para verificar mensagens de email de clientes de email com os quais o AVG é compatível com um plug-in específico, por exemplo, Microsoft Outlook e The Bat*). Ele é usado principalmente com aplicativos de email como Outlook Express, Mozilla, Incredimail etc.

Durante a instalação do , existem servidores automáticos criados para controle de e-mails: um para verificar e-mails de entrada e o segundo para verificar e-mails de saída. Utilizando esses dois servidores, os e-mails são automaticamente verificados nas portas 110 e 25 (*portas padrão para o recebimento e envio de e-mails*).

O Verificador de e-mail funciona como uma interface entre o cliente de e-mail e os servidores de e-mail na Internet.

- ***E-mails de entrada:*** ao receber uma mensagem do servidor, o componente ***Verificador de e-mail*** a testa em busca de vírus, remove anexos infectados e adiciona uma certificação. Quando detectados, os vírus são movidos para a Quarentena de Vírus imediatamente. Então a mensagem é passada para o cliente de e-mail.
- ***E-mails de saída:*** a mensagem é enviada a partir do cliente de e-mail para o Verificador de

e-mail; ele testa essa mensagem e seus anexos em busca de vírus e, em seguida, envia a mensagem ao servidor SMTP (*a verificação de e-mails de saída está desativada por padrão e pode ser configurada manualmente*).

O Verificador de E-mail não se destina a plataformas de servidores.

6.3.2. Anti-spam

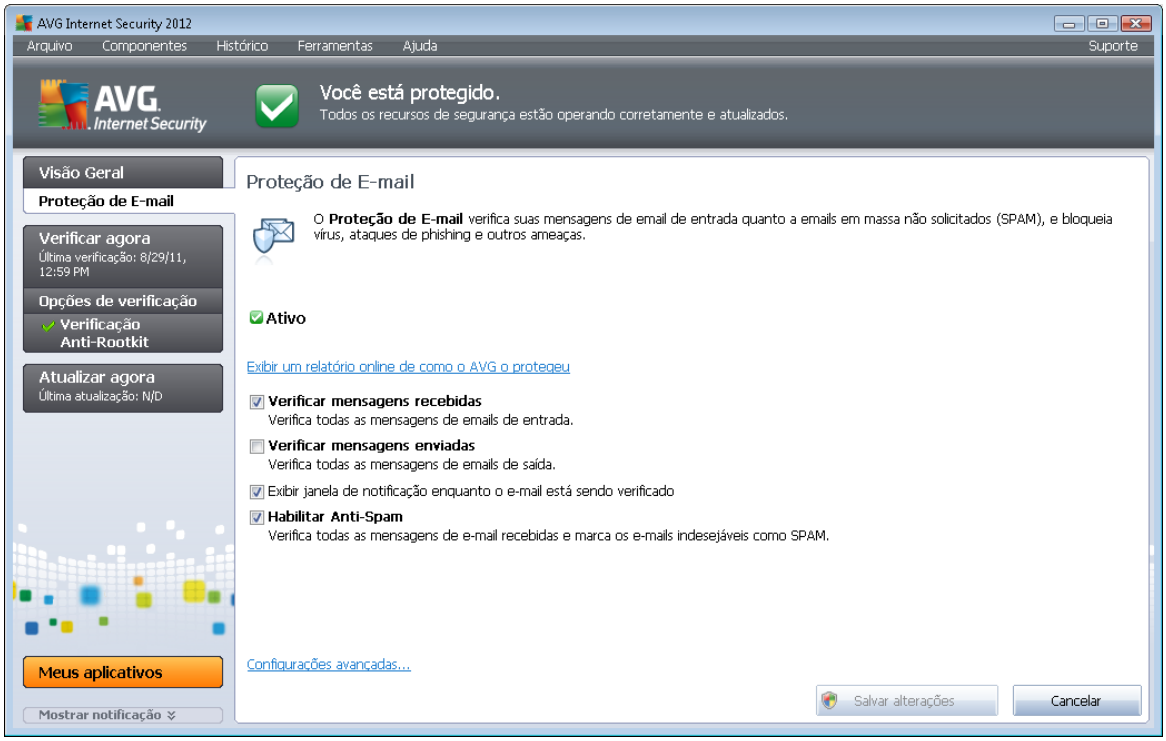
Como funciona o Anti-Spam?

O Anti-Spam verifica todas as mensagens de e-mail recebidas e marca os e-mails indesejáveis como spam. ***O Anti-Spam*** pode modificar o assunto do e-mail (*que foi identificado como spam*), adicionando uma string de texto especial. Dessa forma, é possível filtrar facilmente os seus e-mails no cliente de e-mail. ***O componente Anti-Spam*** usa diversos métodos de análise para processar cada mensagem de e-mail, oferecendo o máximo de proteção possível contra mensagens de e-mail indesejáveis. ***O Anti-Spam*** usa um banco de dados regularmente atualizado para a detecção de spam. Também é possível usar servidores RBL (*bancos de dados públicos de endereços de e-mail de "spammers conhecidos"*) e adicionar manualmente endereços de e-mail à sua Lista de exceções (*nunca marcar como spam*) e à sua Lista negra (*sempre marcar como spam*).

O que é um spam?

Spam refere-se a e-mail não solicitado, a maioria referente a propaganda de produto ou de serviço, enviada em grande quantidade para um grande número de endereços de e-mail ao mesmo tempo, enchendo as caixas de correio. O Spam não se refere a e-mail comercial válido, cujo envio conta com o consentimento por parte dos clientes. O spam não é apenas inoportuno, mas também pode ser fonte de fraudes, vírus ou conteúdo ofensivo.

6.3.3. Interface da Proteção de E-mail



Na caixa de diálogo ***Proteção de E-mail*** , você pode encontrar um breve texto descrevendo a funcionalidade do componente e informações sobre o status atual *(Ativo).* Use o link ***Exibir um relatório online de como o AVG o protegeu*** para examinar as estatísticas detalhadas das atividades e detecções do **AVG Internet Security 2012** em uma página dedicada do site do AVG (http://www.avg.com/).

Configurações básicas da Proteção de E-mail

Na caixa de diálogo ***Proteção de E-mail***, é possível editar algumas funções básicas da funcionalidade do componente:

- ***Verificar mensagens recebidas*** *(ativada por padrão)* - marque este item para especificar que todos os e-mails enviados a sua conta devem ser verificados em busca de vírus.
- ***Verificar mensagens enviadas*** *(desativada por padrão)* - marque o item para confirmar que todos os e-mails enviados pela sua conta devem ser verificados em busca de vírus.
- ***Exibir janela de notificação enquanto o e-mail for verificado*** *(ativada por padrão)* – marque o item para confirmar que deseja ser informado por uma caixa de diálogo de notificação acima do ícone AVG na bandeja do sistema durante a verificação de seu e-mail.
- ***Ativar o Anti-Spam*** *(ativado por padrão)* - marque o item para especificar se deseja que os e-mails recebidos sejam verificados em busca de e-mails não solicitados.

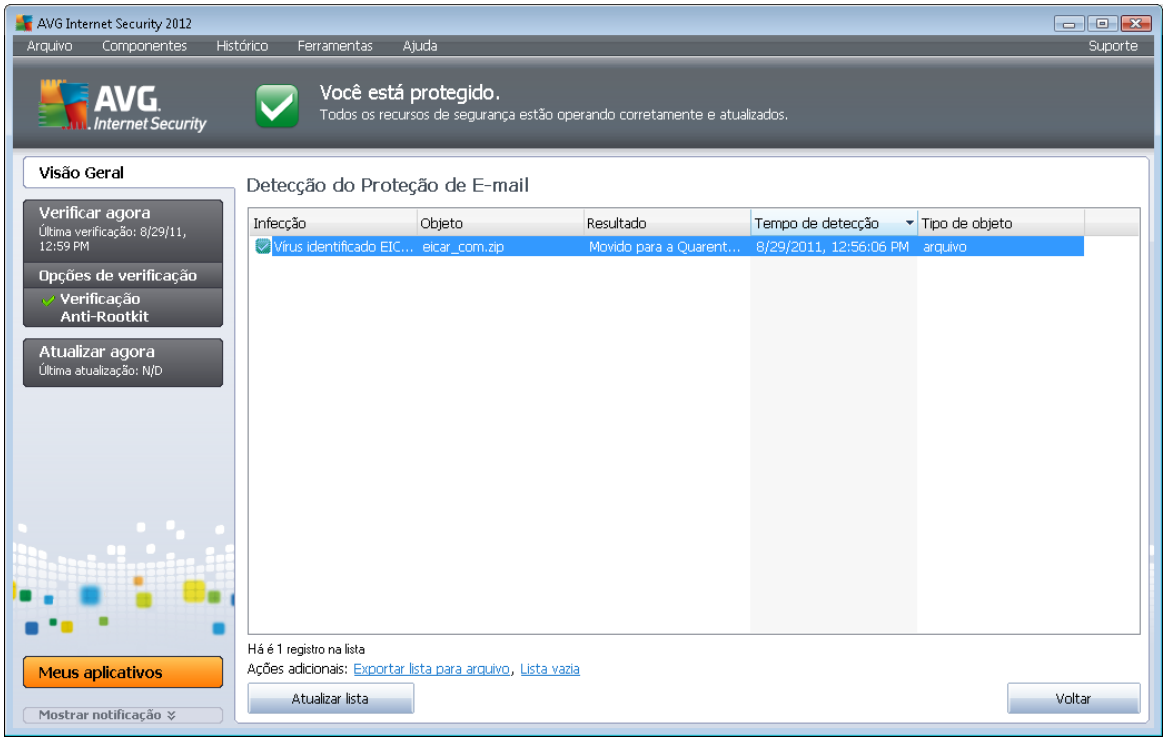
O fornecedor do software configurou todos os componentes do AVG de modo a proporcionar o melhor desempenho possível. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente. Se você precisar alterar a configuração do AVG, selecione o item de menu do sistema Ferramentas/Configurações avançadas e edite a configuração do AVG na caixa de diálogo Configurações avançadas do AVG recém-aberta.

Botões de controle

Os botões de controle disponíveis na caixa de diálogo ***Proteção de E-mail*** são os seguintes:

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione este botão para retornar à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*)

6.3.4. Detecções da Proteção de E-mail



Na caixa de diálogo ***Detecção do Verificador de E-mail*** (*acessada através da opção do menu do sistema Histórico/Detecção do Verificador de E-mail*), é possível ver uma lista de todas as detecções do componente Proteção de E-mail. Em cada objeto detectado, são fornecidas as seguintes informações:

- ***Infecção*** - descrição (possivelmente até o nome) do objeto detectado

- ***Objeto*** - localização do objeto
- ***Resultado*** - ação executada pelo objeto detectado
- ***Hora da detecção*** - data e hora em que o objeto suspeito foi detectado
- ***Tipo de Objeto*** - tipo de objeto detectado

Na parte inferior da caixa de diálogo, na lista, você encontrará informações sobre o total de objetos detectados listados em cima. Além disso você pode exportar a lista inteira de objetos detectados em um arquivo (***Exportar lista para arquivo***) e excluir todas as entradas de objetos detectados (***Lista vazia***).

Botões de controle

Os botões de controle disponíveis na interface de ***Detecção do verificador de e-mail*** são os seguintes:

- ***Atualizar lista*** - atualiza a lista de ameaças detectadas.
- ***Voltar*** - leva você de volta à caixa de diálogo exibida anteriormente.

6.4. Firewall

O firewall é um sistema que impõe uma política de controle de acesso entre duas ou mais redes, bloqueando ou permitindo o tráfego. O Firewall contém um conjunto de regras que protegem a rede interna de ataques originados externamente *(normalmente na Internet)* e controlam toda a comunicação em cada porta da rede. A comunicação é avaliada de acordo com as regras definidas e, então, são permitidas ou proibidas. Se o ***Firewall*** reconhece uma tentativa de invasão, ele "bloqueia" a tentativa e não permite que o invasor acesse o computador.

O firewall é configurado para permitir ou recusar a comunicação interna/externa (de saída ou entrada) por meio de portas definidas e para aplicativos definidos. Por exemplo, o firewall pode ser configurado para permitir que os dados da Web entrem e saiam usando apenas o Microsoft Explorer. Qualquer tentativa de transmitir dados da Web por outro navegador seria bloqueada.

O firewall protege as informações identificadas como pessoais, não permitindo que elas sejam enviadas do seu computador sem permissão. Ele controla a forma como o computador troca dados com outros computadores na Internet ou na rede local. Dentro de uma organização, o ***Firewall*** também protege um único computador de ataques iniciados por usuários internos em outros computadores da rede.

Os computadores que não são protegidos pelo Firewall se tornam um alvo fácil para hackers de computador e roubos de dados.

Recomendação: *geralmente, não é recomendável usar mais de um firewall em um computador individual. A segurança do computador não é aumentada se você instalar mais firewalls. É mais provável que ocorram alguns conflitos entre esses dois aplicativos. Por isso recomendamos que você use somente um firewall no seu computador e desative todos os outros, eliminando assim o risco de possível conflito e de problemas relacionados.*

6.4.1. Princípios do Firewall

No **AVG Internet Security 2012**, o ***Firewall*** controla todo o tráfego em cada porta de rede de seu computador. Com base nas regras definidas, o ***Firewall*** avalia os aplicativos em execução no computador *(e que pretendem se conectar à rede local ou Internet)* ou aplicativos que abordam o computador externamente, tentando estabelecer conexão com o PC. Para cada um desses aplicativos, o ***Firewall*** permitirá ou impedirá a comunicação nas portas da rede. Por padrão, se o aplicativo for desconhecido *(isto é, se não tiver regras definidas de Firewall)*, o ***Firewall*** perguntará se você deseja permitir ou bloquear a tentativa de comunicação.

O Firewall AVG não se destina a plataformas de servidores!

O que o AVG Firewall pode fazer:

- Permitir ou bloquear tentativas de comunicação de aplicativos automaticamente ou pedir sua confirmação
- Usar perfis completos com regras predefinidas, de acordo com as suas necessidades
- Alternar os perfis automaticamente ao se conectar a várias redes ou usar vários adaptadores de rede

6.4.2. Perfis do Firewall

O Firewall permite que você defina regras específicas de segurança com base no fato de o seu computador estar localizado em um domínio, ou ser um computador isolado, ou até mesmo um notebook. Cada uma dessas opções requer um nível diferente de proteção, e os níveis são abordados pelos respectivos perfis. Em suma, um perfil do Firewall é uma configuração específica do componente Firewall e você pode usar várias dessas configurações predefinidas.

Perfis disponíveis

- ***Permitir tudo -***um perfil do sistema de Firewall que foi predefinido pelo fabricante e está sempre presente. Quando esse perfil é ativado, toda a comunicação de rede é permitida e não se aplicam as regras da política de segurança, como se a proteção do Firewall estivesse desativada (isto é, todos os aplicativos são permitidos, mas os pacotes ainda estão sendo verificados; para desabilitar completamente qualquer filtragem, é preciso desabilitar o firewall). Esse perfil do sistema não pode ser duplicado nem excluído e suas configurações não podem ser modificadas.
- ***Bloquear tudo -*** um perfil do sistema de Firewall predefinido pelo fabricante e que está sempre presente. Quando o perfil é ativado, toda a comunicação de rede é bloqueada, e o computador não fica acessível para redes externas, nem pode se comunicar com ambientes externos. Esse perfil do sistema não pode ser duplicado, excluído e suas configurações não podem ser modificadas.
- ***Perfis personalizados*** - os perfis personalizados também permitem que você aproveite o recurso de alternância automática do perfil, que é especialmente útil se você se conecta a várias redes com frequência *(por exemplo, com um notebook)*. Os perfis personalizados

são gerados automaticamente após a instalação do **AVG Internet Security 2012**, atendendo a quaisquer necessidades individuais de regras de política do Firewall. Os seguintes perfis personalizados estão disponíveis:

- ***Diretamente conectado à Internet*** – adequado para notebooks ou computadores domésticos comuns conectados diretamente à Internet sem proteção adicional. Esta opção também é recomendada quando você conecta o notebook a diversas redes desconhecidas e, provavelmente, não seguras (*como em um cyber café, quarto de hotel etc.*).As regras de política de Firewall mais estritas deste perfil garantem que cada computador esteja adequadamente protegida.

- ***Computador no domínio*** – adequado para computadores em uma rede local, geralmente na escola ou no trabalho. Presume-se que a rede esteja administrada profissionalmente e protegida por algumas medidas adicionais, de modo que o nível de segurança pode ser inferior nos casos mencionados acima, permitindo acesso a pastas compartilhadas, unidades de disco, etc.

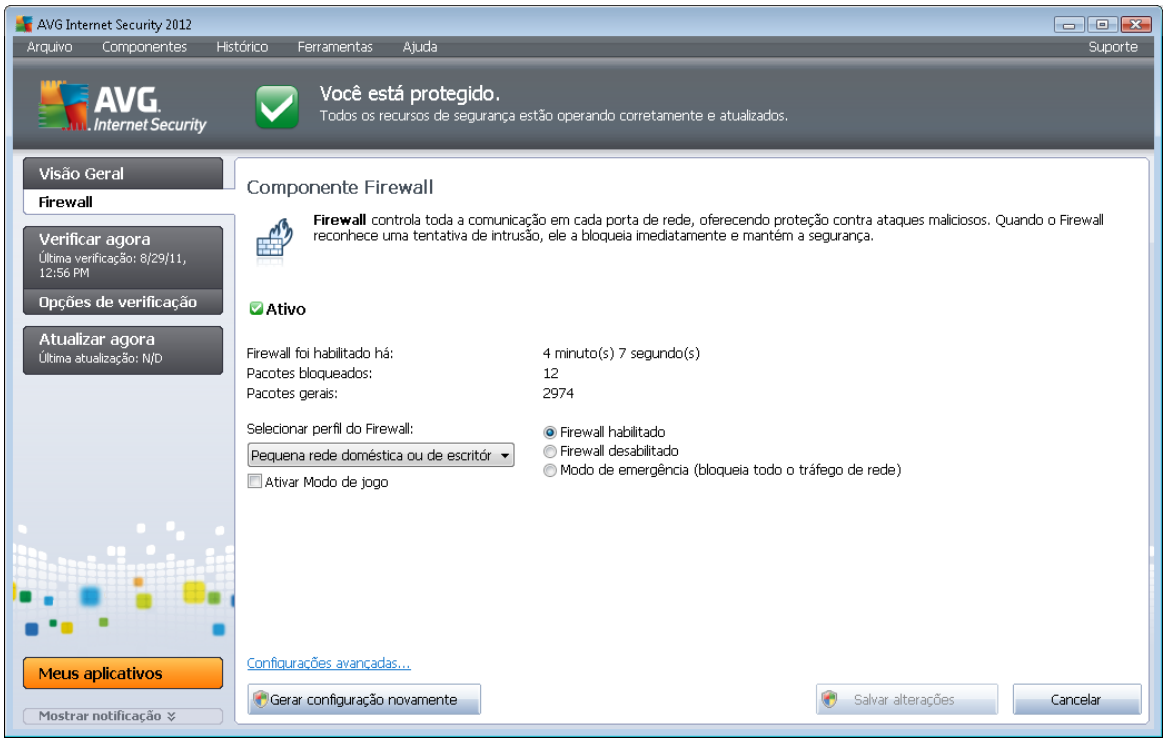
- ***Pequena rede doméstica ou de escritório*** – adequado para computadores em uma rede pequena, geralmente doméstica ou em pequenas empresas. Geralmente, esse tipo de rede não tem administrador "central" e consiste apenas em diversos computadores conectados em conjunto, compartilhando uma impressora, um scanner ou um dispositivo semelhante, o que deve ser refletido nas regras de Firewall.

Alternância de perfil

O recurso Alternância de perfil permite que o Firewall alterne automaticamente para o perfil definido ao usar um determinado adaptador de rede, ou ao se conectar a um determinado tipo de rede. Se nenhum perfil tiver sido atribuído a uma área de rede ainda, durante a próxima conexão com essa área, o Firewall exibirá uma caixa de diálogo solicitando que você atribua um perfil Você pode atribuir perfis para todas as interfaces da rede local ou áreas e especificar futuras configurações na janela Perfis de Áreas e Adaptadores, onde você também pode desabilitar essa função, caso você não deseja utilizá-la (*dessa forma, qualquer tipo de conexão, o perfil padrão será utilizado*).

Geralmente, os usuários que possuem um notebook e usam vários tipos de conexão acharão esse recurso útil. Se você tiver um computador desktop e usar somente um tipo de conexão (*como conexão cabeada à Internet*), não será preciso se preocupar com a alternância de perfil, pois, provavelmente, você nunca a utilizará.

6.4.3. Interface do Firewall



A caixa de diálogo principal nomeada ***Componente Firewall*** fornece informações básicas sobre a funcionalidade do componente, seu status *(Ativo)* e uma breve visão geral das estatísticas do componente:

- ***Firewall foi habilitado há*** - tempo decorrido desde que o Firewall foi iniciado
- ***Pacotes bloqueados*** - número de pacotes bloqueados do volume total de pacotes verificados
- ***Pacotes gerais*** - número de todos os pacotes verificados durante a execução do Firewall

Configurações básicas do Firewall

- ***Selecionar perfil do Firewall*** - no menu suspenso, selecione um dos perfis definidos (*para obter uma descrição detalhada de cada perfil e seu uso recomendado, consulte o capítulo Perfis do Firewall*)
- ***Ativar o Modo de Jogo*** - selecione esta opção para garantir que, quando aplicativos em tela cheia forem executados (*jogos, apresentações, filmes etc.*), o Firewall não exiba caixas de diálogo solicitando se você deseja bloquear ou permitir a comunicação com aplicativos desconhecidos. No caso de um aplicativo desconhecido tentar comunicar-se pela rede neste momento, o Firewall permitirá ou bloqueará a tentativa automaticamente, de acordo com as configurações no perfil atual. ***Nota:*** Quando o modo de jogo está ativado, todas as tarefas programadas (verificações, atualizações) são adiadas até que o aplicativo

seja fechado.

- Além disso, nesta seção de configurações básicas, você pode selecionar três opções alternativas definindo o status atual do componente Firewall:

    - ***Firewall ativado*** *(ativado por padrão)* - selecione esta opção para permitir a comunicação com os aplicativos indicados como "permitidos" no conjunto de regras definidas no perfil selecionado do Firewall.

    - ***Firewall desativado -*** esta opção desativa totalmente o Firewall, todo o tráfego da rede é permitido mas não verificado!

    - ***Modo de emergência (bloquear todo o tráfego de Internet)*** - selecione esta opção para bloquear todo o tráfego em cada porta de rede; o Firewall ainda está em execução, mas todo o tráfego da rede foi interrompido.

Nota: *o fornecedor de software configurou todos os componentes do AVG Internet Security 2012 para que proporcionem um desempenho ideal. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. As alterações nas configurações só devem ser feitas por um usuário experiente. Se você precisar alterar a configuração do Firewall, selecione o item de menu do sistema****Ferramentas/Configurações avançadas*** *e edite a configuração do Firewall na caixa de diálogo recém-aberta Configurações do Firewall.*

Botões de controle

- ***Gerar configuração novamente*** - pressione este botão para substituir a configuração de Firewall existente e reverter para a configuração padrão com base na detecção automática.

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo.

- ***Cancelar*** - pressione este botão para retornar à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*).

6.5. Anti-Rootkit

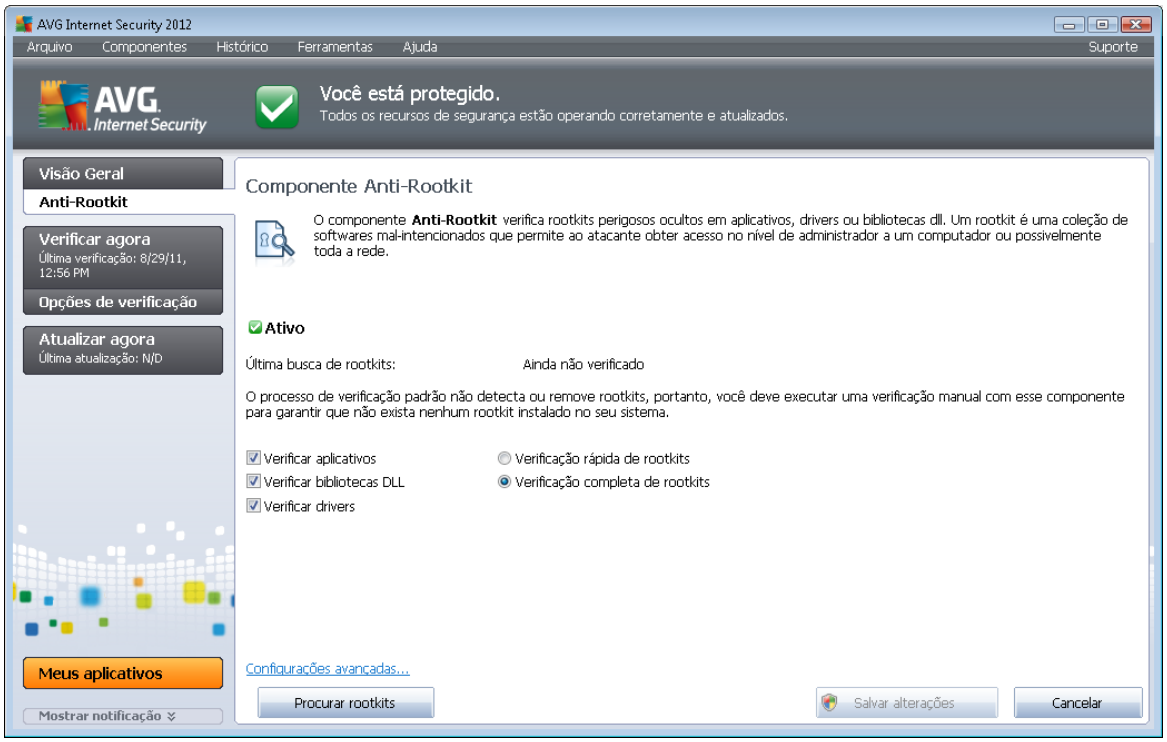
O Anti-Rootkit é uma ferramenta especializada para detectar e remover efetivamente rootkits perigosos, isto é, programas e tecnologias que podem camuflar a presença de software malicioso no seu computador. ***O Anti-Rootkit*** é capaz de detectar rootkits com base em um conjunto de regras predefinidas. Observe que são detectados todos os rootkits *(não apenas os infectados)*. Se o ***Anti-Rootkit*** encontrar um rootkit, isso não quer dizer necessariamente que esse rootkit está infectado. Algumas vezes os rootkits são usados como drivers ou fazem parte de aplicativos corretos.

O que é um rootkit?

Um rootkit é um programa criado para assumir o controle fundamental de um sistema de

computador, sem autorização dos proprietários do sistema e gerentes legítimos. O acesso ao hardware é realmente necessário, pois um rootkit tem o objetivo de executar o controle do sistema operacional executado no hardware. Geralmente, os rootkits atuam para obscurecer sua presença no sistema por meio de subversão ou evasão de mecanismos de segurança padrão do sistema operacional. Freqüentemente, eles também são cavalos-de-tróia, levando os usuários a acreditarem que é confiável executá-los no sistema. As técnicas usadas para conseguir isso podem incluir ocultar processos em execução de programas de monitoramento ou ocultar arquivos ou dados do sistema operacional.

6.5.1. Interface do Anti-Rootkit



A caixa de diálogo ***Anti-Rootkit*** fornece uma breve descrição da funcionalidade do componente, informa o status atual do componente *(Ativo)* e também traz informações sobre a última execução do teste ***Anti-Rootkit*** (***Última busca de rootkits***). A caixa de diálogo ***Anti-Rootkit*** apresenta também o link Ferramentas/Configurações Avançadas. Use o link para ser redirecionado ao ambiente de configuração avançada do componente ***Anti-Rootkit***.

O fornecedor do software configurou todos os componentes do AVG de modo a proporcionar o melhor desempenho possível. A menos que você tenha um motivo real para isso, não mude as configurações do AVG. Alterações nas configurações devem ser realizadas somente por um usuário experiente.

Configurações básicas do Anti-Rootkit

Na parte inferior da caixa de diálogo, você pode configurar algumas funções básicas da verificação de presença de rootkits. Primeiro, marque as respectivas caixas de seleção para especificar objetos

que devem ser verificados:

- ***Verificar aplicativos***
- ***Verificar bibliotecas DLL***
- ***Verificar drivers***

Em seguida, você pode selecionar o modo de verificação do rootkit:

- ***Verificação rápida de rootkits*** - verifica todos os processos em execução, as unidades carregadas e a pasta do sistema (*geralmente c:\Windows*).
- ***Verificação completa de rootkits*** - verifica todos os processos em execução, as unidades carregadas, a pasta do sistema (*tipicamente c:\Windows*), além de todos os discos locais (*incluindo o disco flash, mas excluindo as unidades de CD/disquete*).

Botões de controle

- ***Procurar rootkits*** - como a verificação de rootkits não é parte implícita de Verificar todo o computador, você pode executar a verificação de rootkits diretamente na interface do ***Anti-Rootkit*** usando este botão.
- ***Salvar alterações*** - pressione este botão para salvar todas as alterações feitas nesta interface e voltar para a caixa de diálogo principal padrão do AVG (*visão geral dos componentes*).
- ***Cancelar*** - pressione este botão para voltar à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*) sem salvar as alterações feitas.

6.6. Ferramentas do Sistema

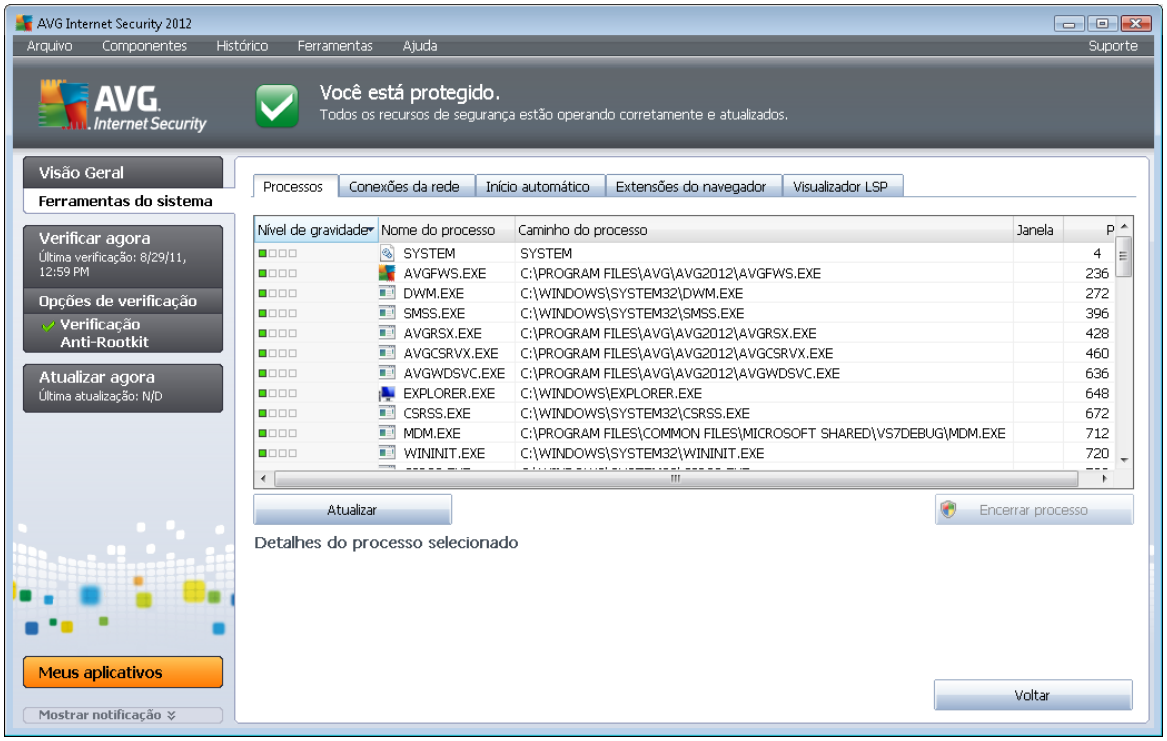
Ferramentas do Sistema refere-se a ferramentas que oferecem um resumo detalhado do sistema operacional e do ambiente do AVG Internet Security 2012. O componente exibe uma visão geral de:

- Processos - lista de processos (*(isto é, aplicativos em execução*) que estão ativos no momento no computador
- Conexões de rede - lista de conexões ativas no momento
- Inicialização automática - lista todos os aplicativos que são executados durante a inicialização do sistema Windows
- Extensões do navegador - lista de plug-ins (*ou seja, aplicativos*) instalados no navegador da Internet
- Visualizador de LSPs - lista de provedores de serviços em camadas (*LSP*)

As visões gerais específicas também podem ser editadas, mas isso é recomendado somente a

usuários bem experientes!

6.6.1. Processos



A caixa de diálogo ***Processos*** contém uma lista de processos (*(isto é, aplicativos em execução)*) que estão ativos no momento no computador. A lista é dividida em várias colunas:

- ***Nível de segurança*** – identificação gráfica da respectiva severidade do processo em uma escala de quatro níveis, variando do menos importante (■□□□) até o mais crítico (■■■■)
- ***Nome do processo*** - nome do processo em execução
- ***Caminho do processo*** - indica um caminho físico para o processo em execução
- ***Janela*** - se aplicável, indica o nome da janela do aplicativo
- ***PID*** - o número de identificação do processo é um identificador exclusivo do processo interno do Windows

Botões de controle

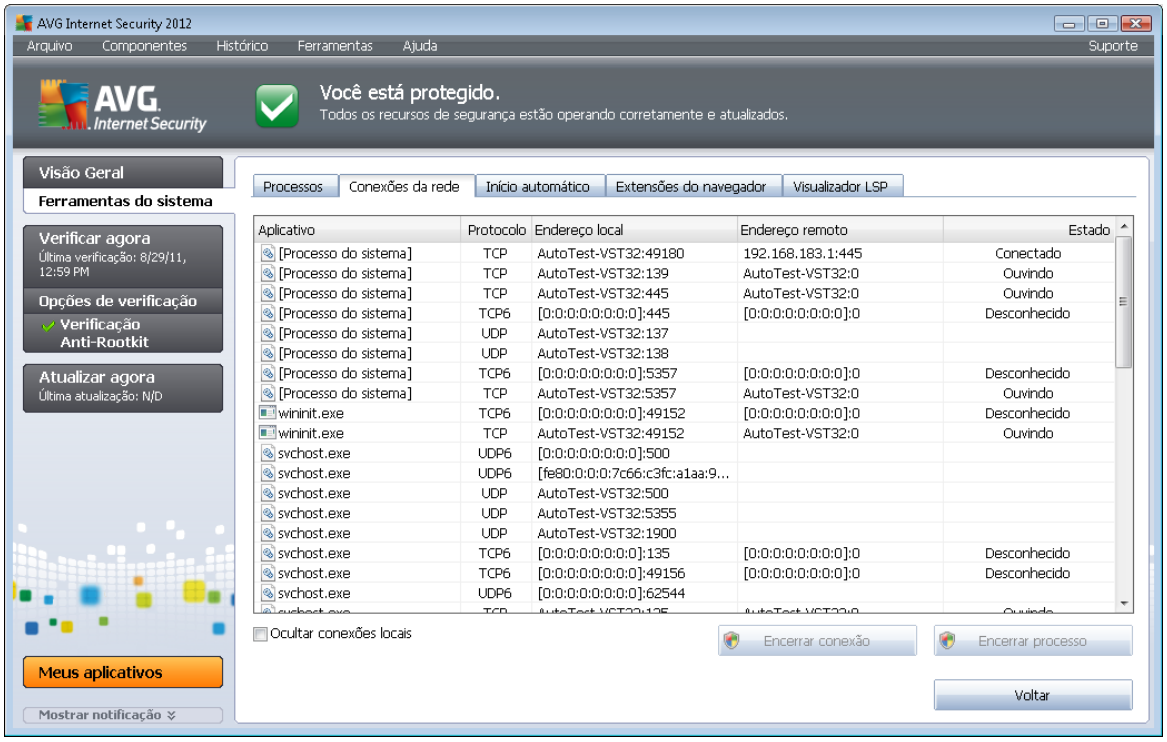
Estes são os botões de controle disponíveis na guia ***Processos***:

- ***Atualizar*** - atualiza a lista de processos de acordo com o status atual
- ***Finalizar processo*** - você pode selecionar um ou mais aplicativos e depois finalizá-los

pressionando esse botão. ***Nós sugerimos não encerrar nenhum aplicativo, a menos que você tenha certeza absoluta de que eles representam uma ameaça real!***

- ***Voltar*** - leva você de volta à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*)

6.6.2. Conexões da Rede



A caixa de diálogo ***Conexões de Rede*** contém uma lista das conexões ativas no momento. A lista é dividida nas seguintes colunas:

- ***Aplicativo*** - nome do aplicativo associado à conexão (*com exceção do Windows 2000 em que as informações não estão disponíveis*)
- ***Protocolo*** - tipo de protocolo de transmissão usado na conexão:
  - TCP - protocolo usado junto com o protocolo de Internet (IP) para transmitir informações pela Internet
  - UDP - alternativa para o protocolo TCP
- ***Endereço local*** - endereço IP do computador local e o número de porta usado
- ***Endereço remoto*** - endereço IP do computador remoto e o número da porta à qual está conectado Se possível, procurará também o nome do host do computador remoto.
- ***Estado*** - indica o estado atual mais provável (*Conectado, Servidor fechado, Escuta, Ativo*

fechado concluído, Passivo fechado, Ativo fechado)

Para listar apenas as conexões externas, marque a caixa de seleção ***Ocultar conexões locais*** na seção inferior da caixa de diálogo, abaixo da lista.

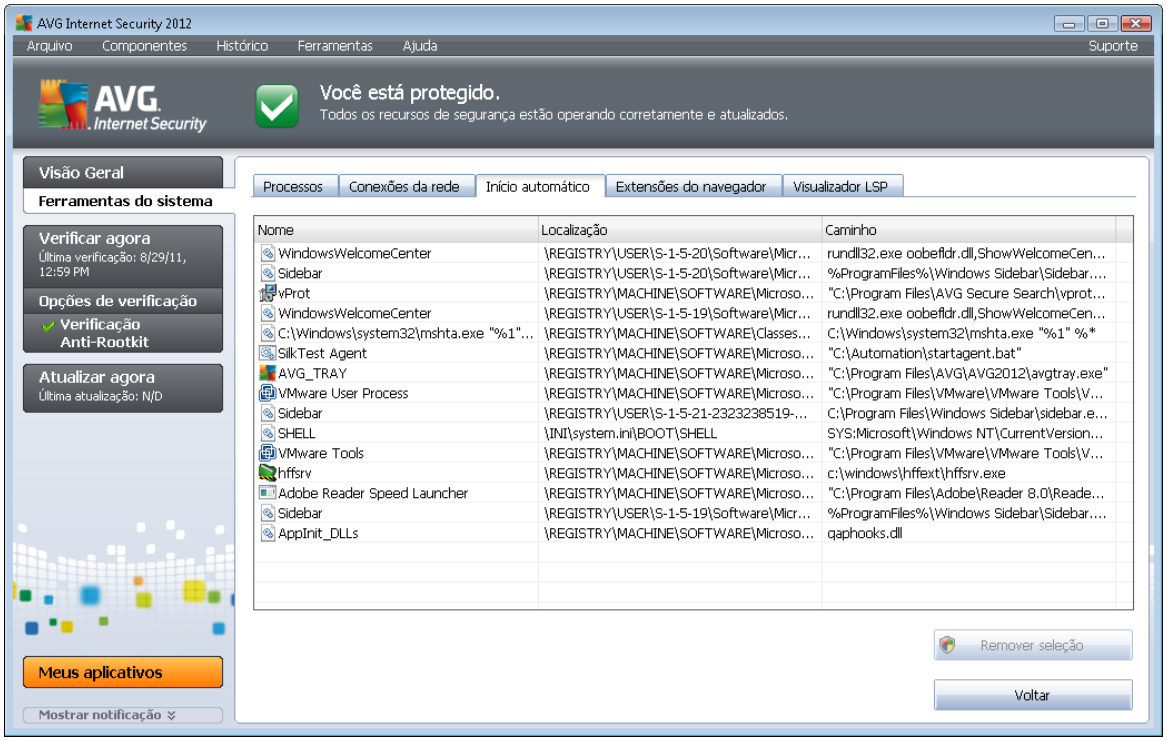
Botões de controle

Estes são os botões de controle disponíveis na guia ***Conexões de rede***:

- ***Encerrar Conexão*** - fecha uma ou mais conexões selecionadas na lista
- ***Terminar processo*** - fecha um ou mais aplicativos associados às conexões selecionadas na lista
- ***Voltar*** - volta para a caixa de diálogo principal padrão do AVG (visão geral dos componentes).

Às vezes só é possível encerrar aplicativos que estejam no estado conectado no momento. Nós sugerimos não encerrar nenhuma conexão, a menos que você tenha certeza absoluta de que elas representam uma ameaça real!

6.6.3. Início automático



A caixa de diálogo ***Inicialização automática*** mostra uma lista de todos os aplicativos executados durante a inicialização do sistema Windows. Muito freqüentemente, vários aplicativos malware são adicionados automaticamente na entrada do registro de inicialização.

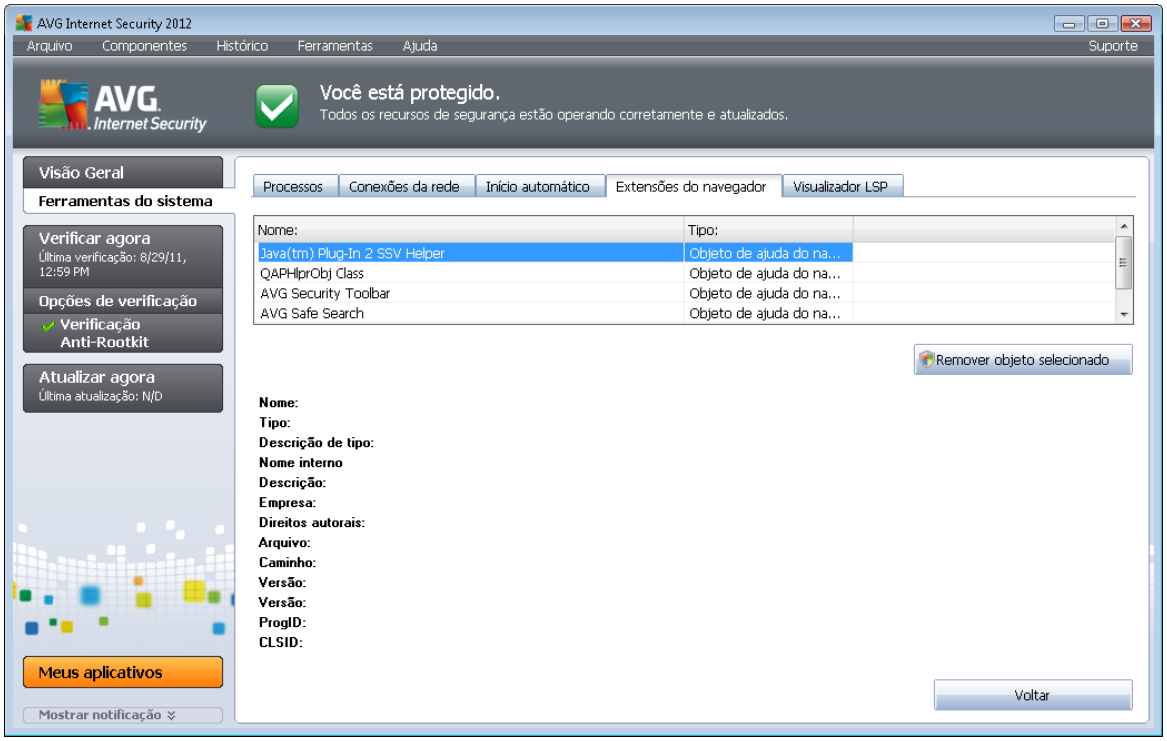
Botões de controle

Estes são os botões de controle disponíveis na guia ***Início automático***:

- ***Remover selecionado*** - pressione o botão para excluir uma ou mais entradas selecionadas.
- ***Voltar*** - retorna à caixa de diálogo principal padrão do AVG *(visão geral dos componentes).*

Nós sugerimos não excluir nenhum aplicativo da lista, a menos que você tenha certeza absoluta de que eles representam uma ameaça real!

6.6.4. Navegador de Extensões



A caixa de diálogo ***Extensões do Navegador*** contém uma lista de plug-ins (*como aplicativos*) instalados no navegador da Internet. Esta lista pode conter os plug-ins normais, assim como programas malware potenciais. Clique em um objeto na lista para obter informações detalhadas sobre o plug-in selecionado que será exibido na seção inferior da caixa de diálogo.

Botões de controle

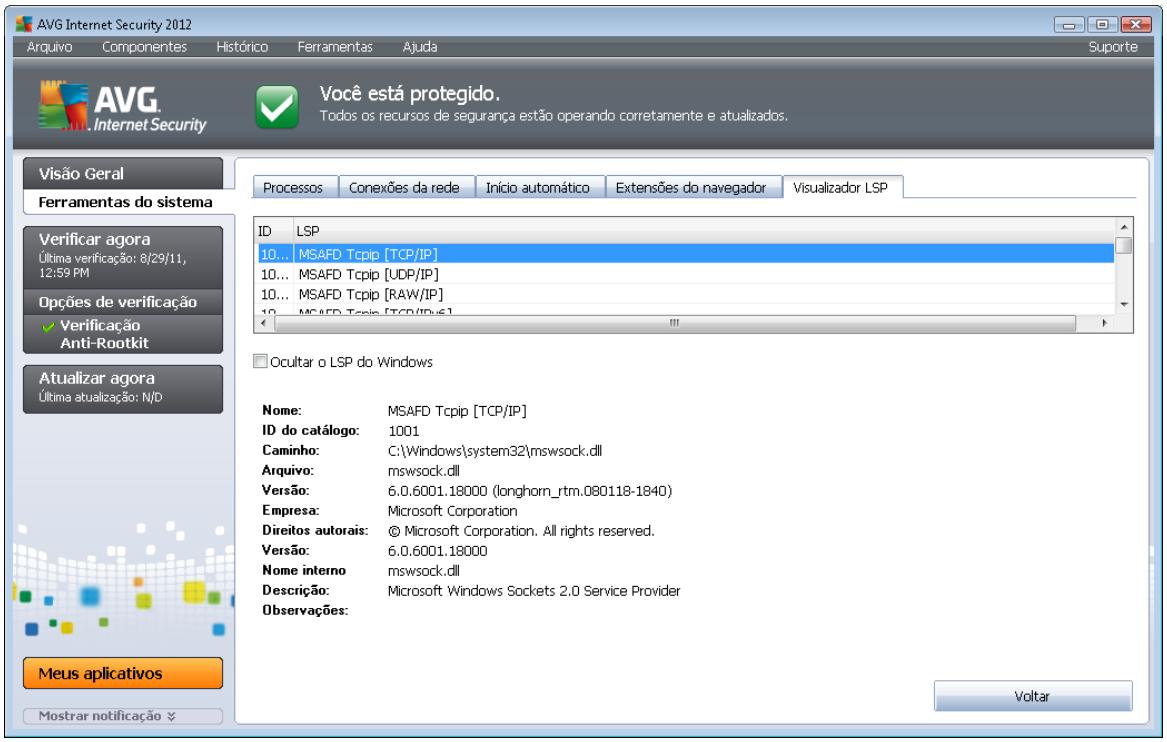
Estes são os botões de controle disponíveis na guia ***Extensões de navegador***:

- ***Remover objeto selecionado*** - remove o plug-in atualmente realçado na lista. ***Nós sugerimos não excluir nenhum plug-in da lista, a menos que você tenha certeza***

absoluta de que eles representam uma ameaça real!

- ***Voltar*** - retorna à caixa de diálogo principal padrão do AVG *(visão geral dos componentes).*

6.6.5. Visualizador LSP



A caixa de diálogo ***Visualizador de LSP*** mostra uma lista de provedores de serviços em camadas (LSP, Layered Service Providers).

Um ***LSP*** é um driver de sistema vinculado aos serviços de rede do sistema operacional Windows. Ele tem acesso a todos os dados enviados e recebidos no computador e pode modificar esses dados. Alguns LSPs são necessários para permitir que o Windows conecte você a outros computadores, inclusive à Internet. No entanto, certos aplicativos malware também podem se instalar como LSPs, tendo acesso a todos os dados transmitidos pelo seu computador. Portanto, essa análise pode ajudá-lo a verificar todas as ameaças de LSP possíveis.

Em determinadas circunstâncias, também é possível reparar LSPs danificados (*por exemplo, quando o arquivo foi removido mas as entradas de registro permanecem intocadas*). Um novo botão para corrigir o problema é exibido quando um LSP reparável é descoberto.

Botões de controle

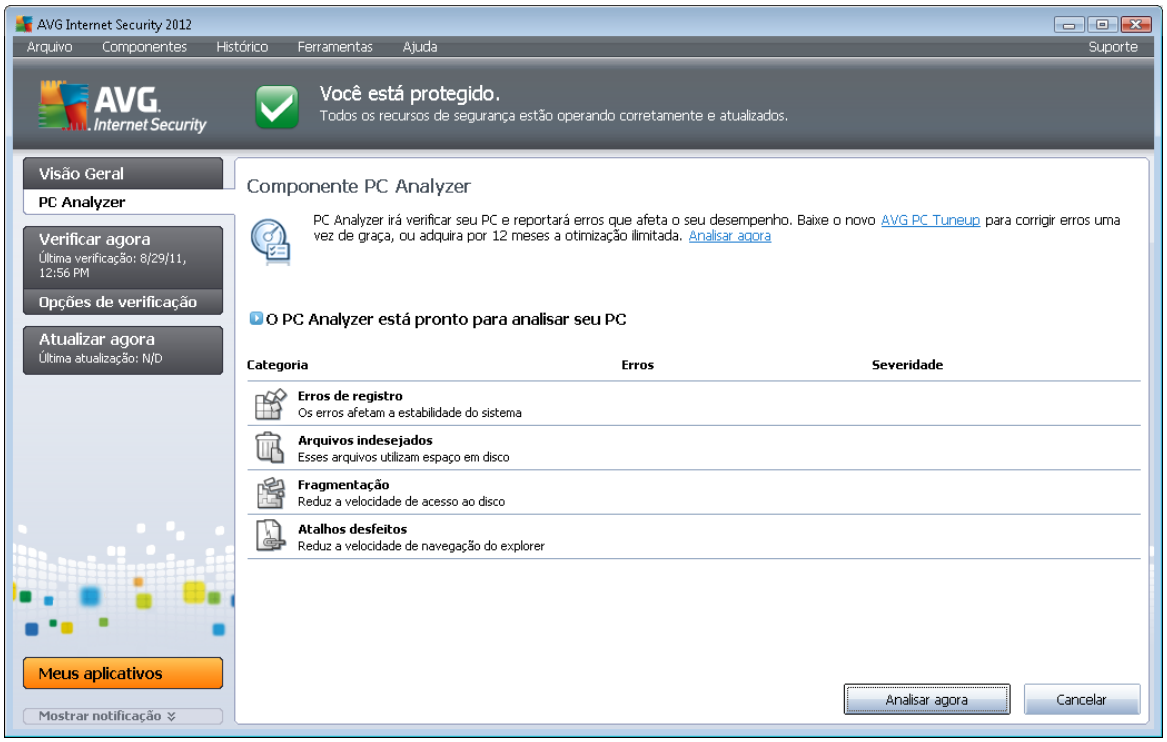
Os botões de controle disponíveis na guia ***Visualizador LSP***são os seguintes:

- ***Ocultar LSP do Windows*** - para incluir o LSP do Windows na lista, desmarque este item.

- ***Voltar*** - leva você de volta à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*).

6.7. PC Analyzer

O componente ***PC Analyzer*** verifica o seu computador quanto a problemas de sistema e apresenta uma visão geral transparente do que pode estar afetando o desempenho geral do computador. Na interface do usuário do componente, é possível ver um gráfico dividido em quatros linhas relacionadas às respectivas categorias:



- ***Erros do Registro*** exibirá o número de erros no Registro do Windows. Como corrigir o Registro requer conhecimento avançado, não é recomendável que você tente corrigi-lo sozinho.

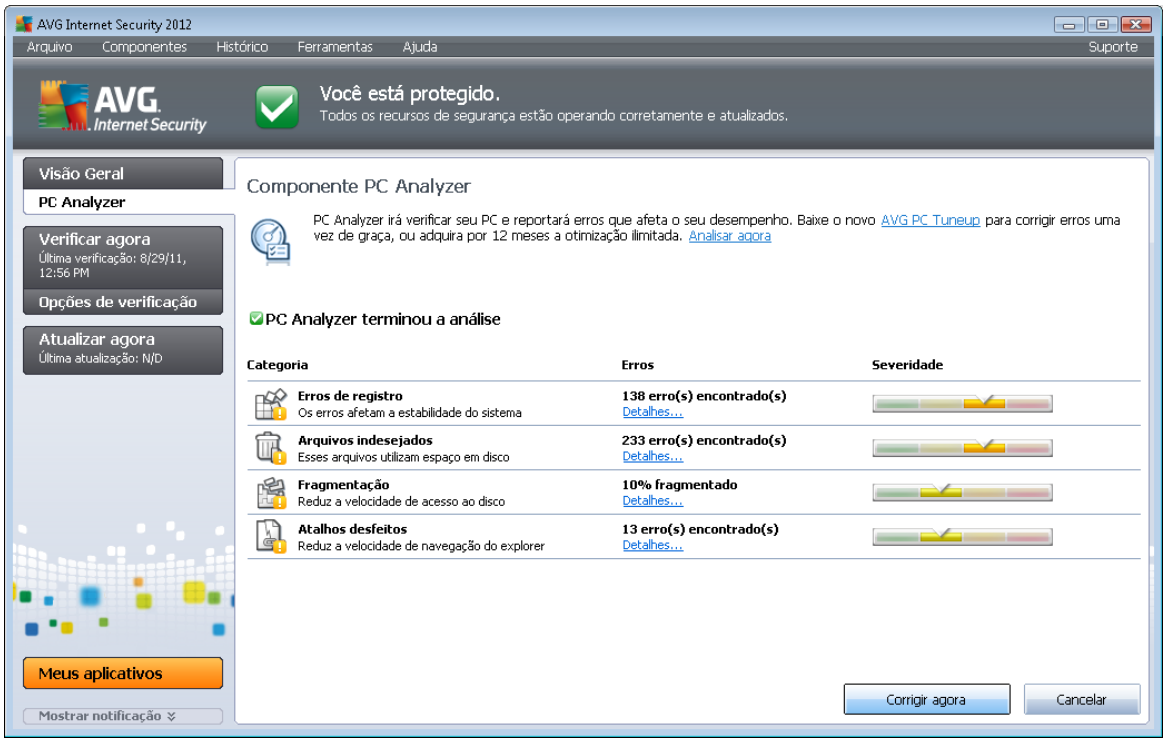
- ***Arquivos indesejados*** exibirá o número de arquivos que muito provavelmente podem ser gerados externamente. Geralmente, há muitos tipos de arquivos temporários e arquivos na Lixeira.

- ***A Fragmentação*** calculará a porcentagem de disco rígido que está fragmentada, ou seja, usada por muito tempo, fazendo com que a maioria dos arquivos esteja espalhada por diferentes partes do disco físico. Você pode usar uma ferramenta de desfragmentação para corrigir isso.

- ***Atalhos desfeitos*** notificará você sobre atalhos que não funcionam mais, que levam a locais não existentes, etc.

Para iniciar a análise do seu sistema, pressione o botão ***Analisar agora***. Você poderá acompanhar

o progresso da análise e os seus resultados diretamente no gráfico:



A visão geral de resultados apresenta o número de problemas de sistema detectados (***Erros***) divididos de acordo com as respectivas categorias testadas. Os resultados da análise serão também exibidos graficamente em um eixo na coluna ***Gravidade*** .

Botões de controle

- ***Analisar agora*** (*exibido antes do início da análise*) - press este botão para iniciar a análise imediata do seu computador
- ***Corrigir agora*** (*exibição única quando a análise é finalizada*) - pressione o botão para acessar o site do AVG (http://www.avg.com/) na página que fornece informações detalhadas e atualizadas relacionadas ao componente ***PC Analyzer***
- ***Cancelar*** - pressione este botão para interromper a análise em execução ou retornar à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*) quando a análise for concluída

6.8. Identity Protection

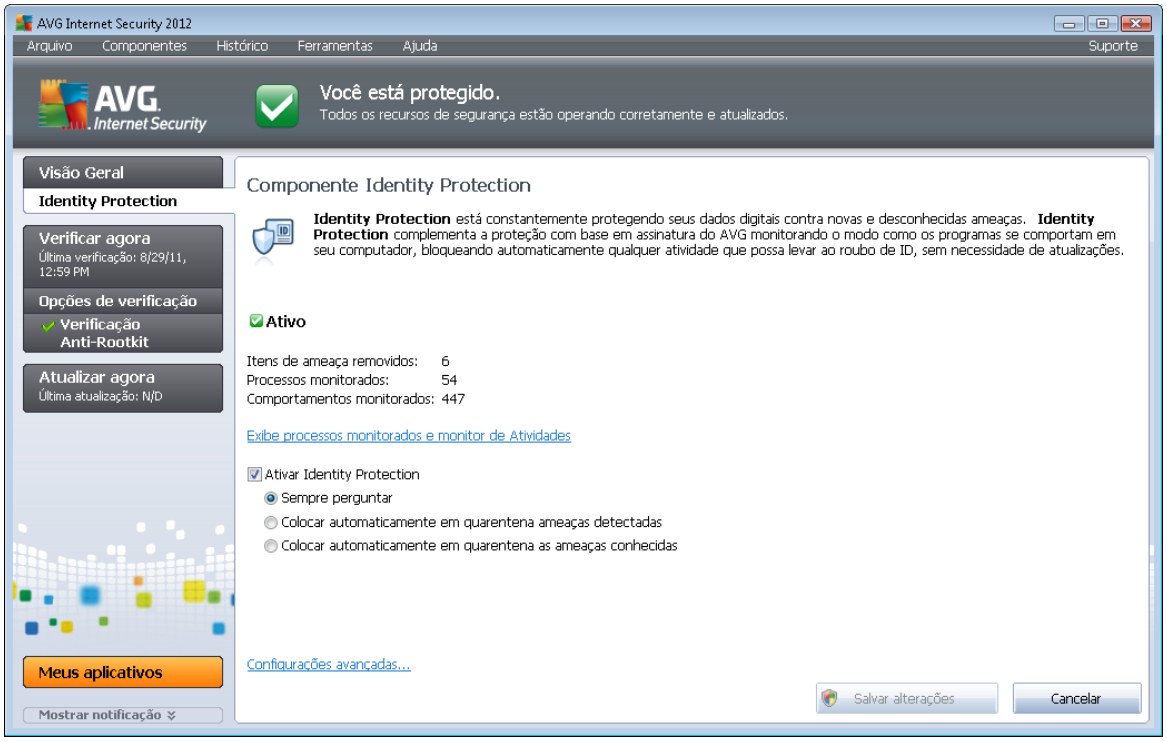
O Identity Protection é um componente anti-malware que o protege de todos os tipos de malware (*spyware, robôs, roubo de identidade...*) usando tecnologias comportamentais e que fornece proteção imediata contra novos vírus. ***O foco do Identity Protection é evitar que ladrões de identidade roubem suas senhas, informações de conta bancária, números de cartões de crédito e outros dados pessoais digitais a partir de todos os tipos de software malicioso***

(malware) que visam ao seu PC. Ele garante que todos os programas em execução no seu PC estejam funcionando corretamente. ***O Identity Protection***aponta e bloqueia comportamento suspeito em base contínua, além de proteger seu computador de todos os novos malware.

O Identity Protection fornece proteção em tempo real ao seu computador contra ameaças novas e, até mesmo, desconhecidas. Ele monitora todos os processos *(incluindo os ocultos)* e mais de 285 padrões de comportamentos diferentes, assim como pode determinar se algo mal-intencionado está ocorrendo em seu sistema. Por isso, pode revelar ameaças ainda não descritas no banco de dados de vírus. Quando um código desconhecido chega ao seu computador, é imediatamente vigiado por comportamento malicioso e monitorado. Se o arquivo for considerado mal-intencionado, o ***Identity Protection*** removerá o código para a Quarentena de vírus e reverterá todas as alterações que foram feitas no sistema *(injeções de código, mudanças no registro, abertura de portas etc.)*. Não é preciso iniciar uma verificação para estar protegido. A tecnologia é muito pró-ativa, raramente precisa ser atualizada e está sempre de prontidão.

O Identity Protection é uma proteção complementar ao Antivírus. Recomendamos que você tenha ambos os componentes instalados, de modo a obter proteção total para seu PC.

6.8.1. Interface da Proteção de Identidade



A caixa de diálogo ***Identity Protection*** fornece uma breve descrição da funcionalidade básica do componente, seu status *(Ativo)* e alguns dados estatísticos:

- ***Itens de ameaças removidas*** - fornece o número de aplicativos detectados como malware e removidos
- ***Processos monitorados*** - número de aplicativos atualmente em execução que estão sendo monitorados pelo IDP

- ***Comportamentos monitorados*** - número de ações específicas em execução com os aplicativos monitorados

Abaixo, você pode encontrar o link Exibir processos monitorados e monitor de Atividades, que o levará para a interface do usuário do componente Ferramentas do sistema, em que é possível localizar uma visão geral detalhada de todos os processos monitorados.

Configurações básicas do Identity Protection

Na parte inferior da caixa de diálogo, você pode editar alguns recursos básicos da funcionalidade do componente:

- ***Ativar Identity Protection*** - (*ativada por padrão*): marque para ativar o componente IDP e abrir opções de edição adicionais.

  Em alguns casos, o ***Identity Protection*** pode relatar que alguns arquivos autênticos são suspeitos ou perigosos. Como o ***Identity Protection*** detecta ameaças com base em seu comportamento, isso normalmente ocorre quando algum programa tenta controlar as teclas, instalar outros programas ou quando um novo driver é instalado no computador. Portanto, selecione uma das opções a seguir, que especificam o comportamento do componente ***Identity Protection*** se ele detectar uma atividade suspeita:

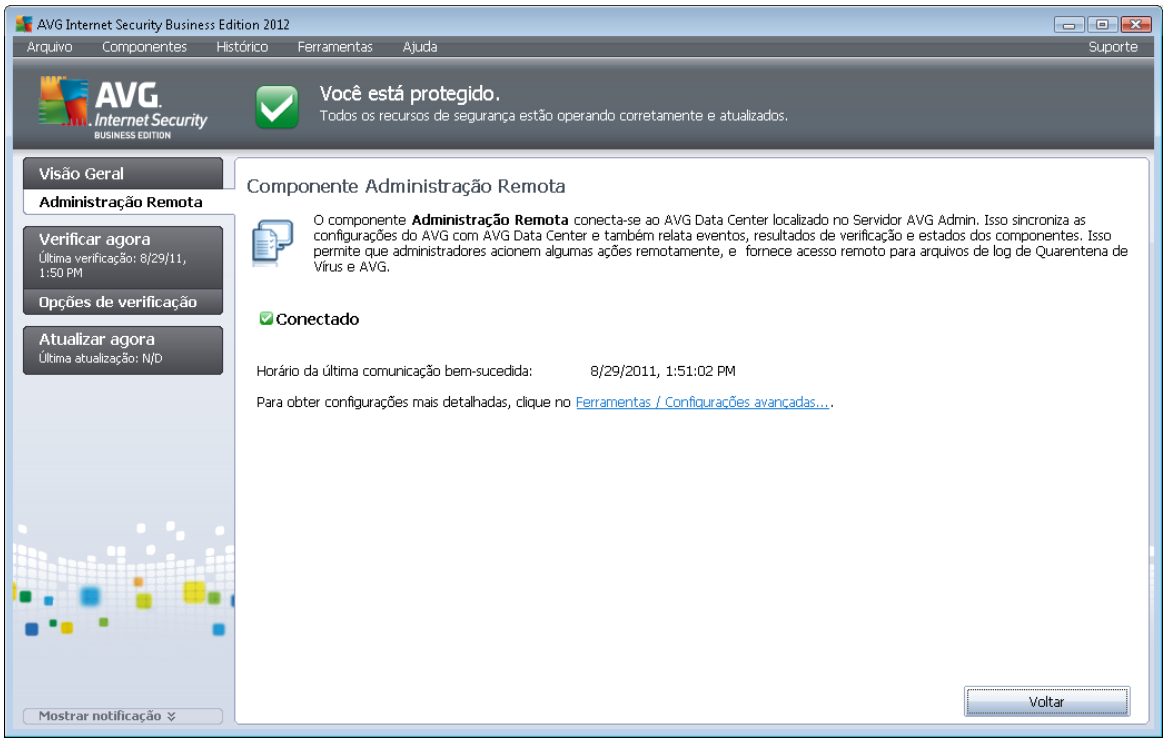
  - ***Sempre avisar***- se um aplicativo for detectado como malware, você deverá determinar se ele deve ou não ser bloqueado (*essa opção está ativada por padrão, e convém não alterá-la, a não ser que você tenha um motivo concreto para isso*)
  - ***Colocar ameaças detectadas automaticamente em quarentena*** - todos os aplicativos detectados como malware serão bloqueados automaticamente
  - ***Colocar ameaças detectadas automaticamente em quarentena*** - todos os aplicativos detectados com certeza absoluta como malware serão bloqueados

Botões de controle

Os botões de controle disponíveis na interface do ***Identity Protection*** são os seguintes:

- ***Salvar alterações*** - pressione este botão para salvar e aplicar quaisquer alterações feitas na caixa de diálogo
- ***Cancelar*** - pressione este botão para voltar para a caixa de diálogo principal padrão do AVG (*visão geral dos componentes*)

6.9. Administração Remota



O componente ***Administração Remota*** é exibido na interface de usuário do **AVG Internet Security 2012** apenas se você tiver instalado a Business Edition do produto *(para obter informações sobre a licença usada na instalação, consulte a guia Versão da caixa de diálogo Informações, que pode ser acessada pelo item de menu do sistema Suporte)*. Na caixa de diálogo ***Componente de Administração Remota***, você pode encontrar informações relativas ao componente, ou seja, se ele está ativo e conectado ao servidor. Todas as configurações do componente ***Administração Remota*** devem ser feitas em ***Configurações Avançadas/Administração Remota***.

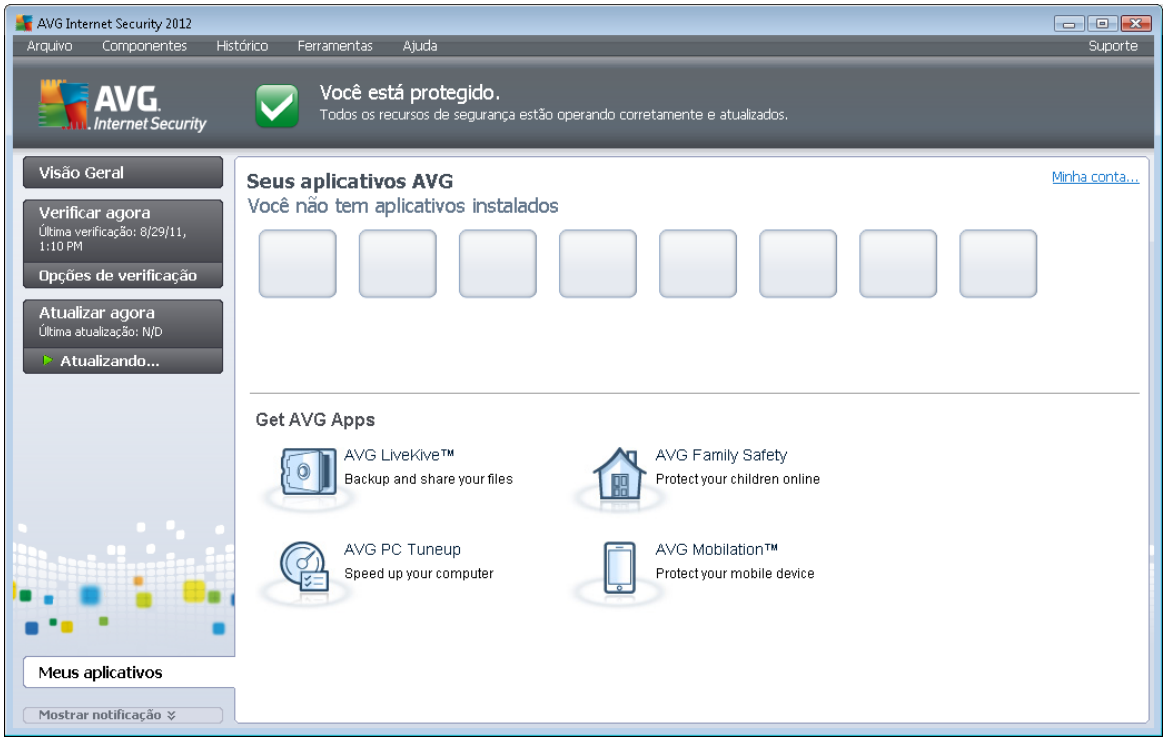
Para obter uma descrição detalhada das opções e da funcionalidade do componente no sistema Administração Remota do AVG, consulte a documentação específica dedicada a esse tópico exclusivamente. Esta documentação está disponível para download no site do AVG (http://www.avg.com/), na seção ***Centro de suporte/Download/Documentação***.

Botões de controle

- ***Voltar*** - pressione este botão para voltar à caixa de diálogo principal padrão do AVG (*visão geral dos componentes*).

7. Meus aplicativos

Os três aplicativos do LiveKive, Family Safety e PC Tuneup estão disponíveis como produtos autônomos do AVG e como parte opcional de sua instalação do **AVG Internet Security 2012**. Na caixa de diálogo ***Seus aplicativos do AVG*** *(que pode ser acessada por meio do botão Meus aplicativos, diretamente na caixa de diálogo principal do AVG)*, você pode obter uma visão geral dos aplicativos que já estão instalados e prontos para serem instalados opcionalmente:



7.1. LiveKive

O LiveKive se dedica a fazer backup de dados online em servidores seguros. ***O LiveKive*** faz backup automático de todos os arquivos, fotos e músicas em um local seguro, permitindo que você os compartilhe com a família e amigos e os acesse de qualquer dispositivo habilitado da web, incluindo dispositivos iPhones e Android. Os recursos do ***LiveKive*** incluem:

- Medida de segurança em caso do computador e/ou disco rígido for corrompido
- Acesse seus dados de qualquer dispositivo conectado à Internet
- Fácil organização
- Compartilhamento com qualquer pessoa que você autorizar

Para obter informações detalhadas, visite a página da Web dedicada do AVG, onde você também pode baixar o componente imediatamente. Para isso, você pode usar o link LiveKive na caixa de diálogo Meus aplicativos.

7.2. Family Safety

A Proteção para a Família ajuda a proteger seus filhos contra conteúdo de mídia, pesquisas on-line e sites inapropriados, além de enviar relatórios sobre as atividades que eles realizam on-line. Você pode definir o nível apropriado de proteção para cada um de seus filhos e monitorá-los individualmente por meio de logins exclusivos.

Para obter informações detalhadas, visite a página da Web dedicada do AVG, onde você também pode baixar o componente imediatamente. Para isso, você pode usar o link Family Safety na caixa de diálogo Meus aplicativos.

7.3. PC Tuneup

O aplicativo ***PC Tuneup*** é uma ferramenta avançada para correção e análise detalhada do sistema, tendo como objetivo o aprimoramento da velocidade e do desempenho geral de seu computador. ***O PC Tuneup*** oferece os seguintes recursos:

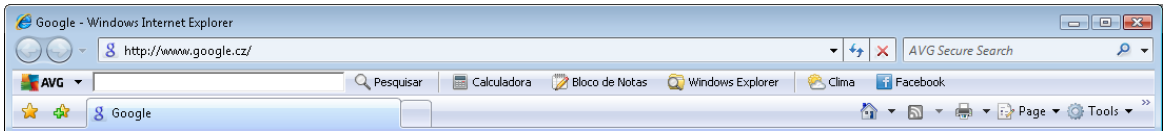
- Disk Cleaner - remove arquivos desnecessários que deixam o computador lento.
- Disk Defrag - desfragmenta as unidades de disco e otimiza a localização dos arquivos do sistema.
- Registry Cleaner - repara erros de registro para aumentar a estabilidade do PC.
- Registry Defrag - compacta o registro, eliminando lacunas que consomem a memória.
- Disk Doctor - busca setores defeituosos, clusters perdidos e erros de diretório, corrigindo-os.
- Internet Optimizer - ajusta as configurações gerais para uma determinada conexão à Internet.
- Track Eraser - remove o histórico de utilização do computador e da Internet.
- Disk Wiper - apaga espaço livre nos discos para impedir a recuperação de dados confidenciais.
- File Shredder - apaga os arquivos selecionados para não serem recuperados em um disco ou uma unidade USB.
- File Recovery - recupera arquivos que foram excluídos acidentalmente em discos, unidades USB ou câmeras.
- Duplicate File Finder - ajuda a localizar e remover arquivos duplicados que desperdiçam espaço em disco.
- Services Manager - desabilita serviços desnecessários que deixam o computador lento.
- Startup Manager - permite que um usuário gerencie os programas que são iniciados automaticamente quando o Windows é inicializado.

- Uninstall Manager - desinstala por completo os programas de software que você não usa mais.
- Tweak Manager - permite que um usuário ajuste centenas de configurações ocultas do Windows.
- Task Manager - lista todos os processos, serviços e arquivos bloqueados em execução.
- Disk Explorer - mostra os arquivos que ocupam mais espaço em um computador.
- System Information - fornece informações detalhadas sobre o hardware e software instalados.

Para obter informações detalhadas, visite a página dedicada da AVG, onde também é possível fazer o download imediato do componente. Para fazer isso, use o link para o PC Tuneup na caixa de diálogo Meus aplicativos.

8. Barra de Ferramentas de Segurança do AVG

A Barra de Ferramentas de Segurança do AVG é uma ferramenta que trabalha em conjunto com o componente LinkScanner, oferecendo segurança máxima enquanto você navega na Internet. No **AVG Internet Security 2012**, a instalação da ***Barra de Ferramentas de Segurança do AVG*** é opcional. Durante o processo de instalação você é convidado a optar pela instalação ou não do componente. ***A Barra de Ferramentas de Segurança do AVG*** está disponível diretamente no navegador da Internet. No momento, os navegadores da Internet suportados são o Internet Explorer (*versão 6.0 e mais recente*) e Mozilla Firefox (*versão 3.0 e mais recente*). Nenhum outro navegador é suportado *(se você estiver usando um navegador da Internet alternativo, como o Avant Browser, poderá perceber um comportamento inesperado)*.



A Barra de Ferramentas de Segurança do AVG consiste no seguinte:

- ***Logotipo do AVG*** com o menu suspenso:
  - ***Usar AVG Secure Search*** - permite pesquisar diretamente na ***Barra de Ferramentas de Segurança do AVG*** usando o mecanismo ***AVG Secure Search***. Todos os resultados da pesquisa são verificados de maneira contínua pelo serviço Search-Shield, permitindo que você se sinta totalmente seguro online.
  - ***Nível atual de ameaças*** - abre a página da Web do laboratório de vírus AVG, com uma exibição gráfica do nível atual de ameaças na Web.
  - ***AVG Threat Labs*** - abre a página ***Relatórios do Site*** no site do AVG (http://www.avg.com/), onde você pode pesquisar ameaças específicas por nome e obter informações detalhadas sobre cada uma.
  - ***Ajuda da Barra de Ferramentas*** - abre a ajuda online, cobrindo todos os recursos da ***Barra de Ferramentas de Segurança do AVG***.
  - ***Enviar feedback de produto*** - abre uma página da Web com um formulário que você pode preencher e nos contar sua opinião sobre a ***Barra de Ferramentas de Segurança do AVG***.
  - ***Sobre...*** - abre uma nova janela com informações sobre a versão da ***Barra de Ferramentas de Segurança do AVG*** instalada no momento.
- ***Campo Pesquisar*** - faça pesquisas na Internet usando a ***Barra de Ferramentas de Segurança do AVG*** para ficar totalmente seguro e confortável, já que todos os resultados de pesquisa exibidos são completamente seguros. Digite uma palavra-chave ou expressão no campo de pesquisa e clique no botão ***Pesquisar*** *(ou pressione Enter)*. Todos os resultados da pesquisa são verificados continuamente pelo serviço Search-Shield *(no componente LinkScanner)*.
- Botões de atalho para o acesso rápido a esses aplicativos: ***Calculadora***, ***Bloco de Notas***,

Windows Explorer

- ***Tempo*** - o botão abre uma nova caixa de diálogo que fornece informações sobre o tempo em seu local e sobre a previsão meteorológica para os dois próximos dias. Essas informações são atualizadas regularmente de cada 3 a 6 horas. Na caixa de diálogo, você pode alterar o local desejado manualmente e decidir se deseja ver informações sobre a temperatura em Celsius ou Fahrenheit.

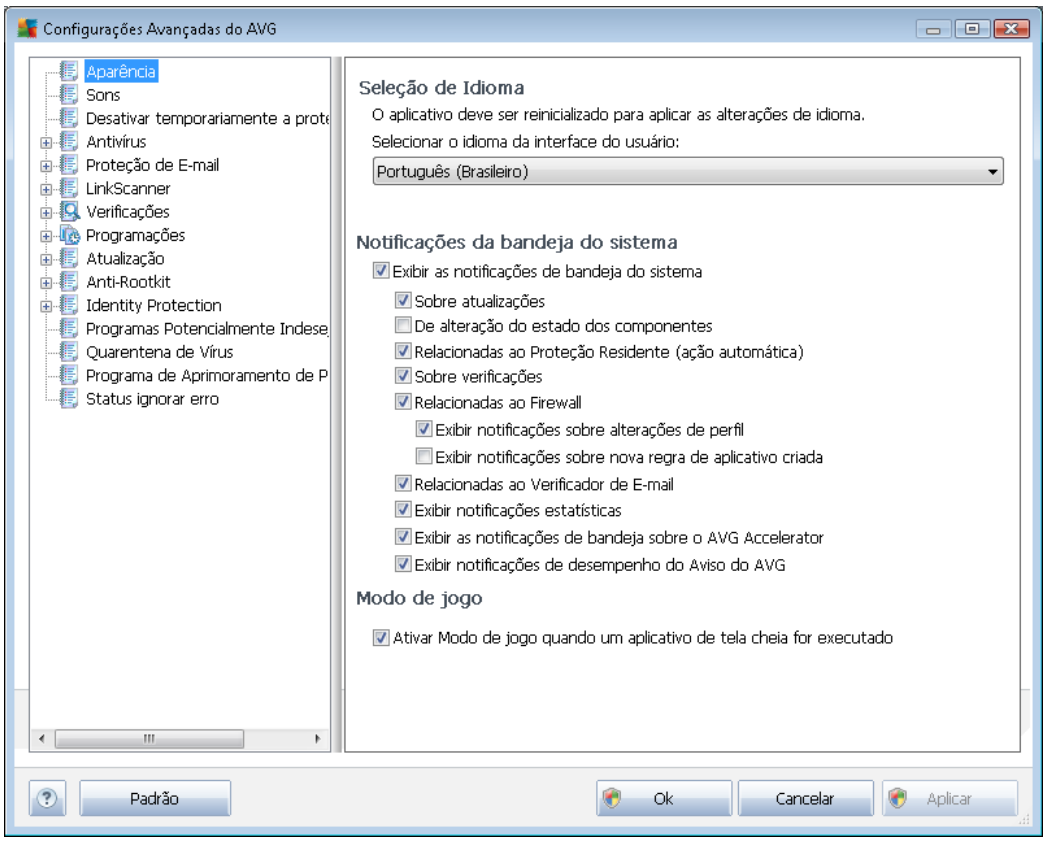
- ***Facebook*** - este botão permite que você se conecte à rede social Facebook diretamente a partir da ***Barra de Ferramentas de Segurança do AVG***. *comportamento.*

9. Configurações Avançadas do AVG

A caixa de diálogo de configuração avançada do **AVG Internet Security 2012** é aberta em uma nova janela denominada ***Configurações Avançadas do AVG***. A janela é dividida em duas seções: a parte da esquerda oferece uma navegação organizada em árvore para as opções de configuração do programa. Selecione o componente do qual deseja alterar a configuração do (*ou sua parte específica*) para abrir a caixa de edição na seção à direita da janela.

9.1. Aparência

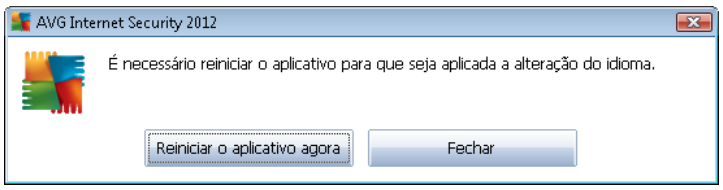
O primeiro item na árvore de navegação, ***Aparência***, refere-se às configurações gerais da interface de usuário do **AVG Internet Security 2012** e fornece algumas opções básicas do comportamento do aplicativo:



Seleção de idioma

Na seção ***Seleção de idioma***, você pode selecionar o idioma desejado no menu suspenso. O idioma selecionado será usado em toda a interface de usuário do **AVG Internet Security 2012**. O menu suspenso oferece apenas os idiomas selecionados anteriormente para serem instalados durante o processo de instalação (*consulte o capítulo Opções personalizadas*), além do inglês (*que é sempre instalado automaticamente*). Para concluir a mudança de idioma do **AVG Internet Security 2012** , é necessário reiniciar o aplicativo. Por favor siga esses passos:

- No menu suspenso, selecione o idioma desejado para o aplicativo
- Confirme a seleção clicando no botão ***Aplicar*** *(canto inferior direito da caixa de diálogo)*
- Pressione o botão ***OK*** para confirmar
- Uma nova caixa de diálogo é exibida informando que, para mudar o idioma do aplicativo, é necessário reiniciar o **AVG Internet Security 2012**
- Clique no botão ***Reiniciar o aplicativo agora*** para concordar com o reinício do programa e aguarde um pouco até que a mudança de idioma seja efetuada:



Notificações da bandeja do sistema

Nesta seção, é possível ocultar as notificações na bandeja do sistema sobre o status do aplicativo **AVG Internet Security 2012**. Por padrão, as notificações do sistema podem ser exibidas. Recomenda-se manter essa configuração. As notificações do sistema informam, por exemplo, sobre o início de processos de atualização ou verificação ou sobre a mudança de status de um componente do **AVG Internet Security 2012** . É necessário prestar atenção a esses anúncios!

Entretanto, se, por alguma razão, você decidir que não deseja receber as informações dessa forma ou que gostaria de receber apenas algumas notificações *(relacionadas a um componente específico do AVG Internet Security 2012)*, poderá definir e especificar suas preferências marcando/ desmarcando as seguintes opções:

- ***Exibir as notificações de bandeja do sistema*** *(ativada por padrão)* - todas as notificações são exibidas por padrão. Desmarque este item para desativar completamente a exibição de todas as notificações do sistema. Quanto ativado, é possível selecionar quais notificações específicas devem ser exibidas:
  - ***Exibir notificações da bandeja sobre atualizações*** *(ativada por padrão)* - decida se as informações relacionadas ao início, andamento ou à finalização do processo de atualização do **AVG Internet Security 2012** devem ser exibidas.
  - ***Exibir notificações de alteração do estado dos componentes*** *(desativada, por padrão)* - decida se devem ser exibidas informações referentes à atividade/inatividade de componentes ou a possíveis problemas. Ao relatar o status de falha de um componente, esta opção se iguala à função informativa do ícone na bandeja do sistema, informando um problema em qualquer componente do **AVG Internet Security 2012**.
  - ***Exibir notificações da bandeja relacionadas à Proteção Residente (ação automática)*** *(ativada por padrão)* - decida se as informações relacionadas a salvar,

copiar e abrir processos devem ser exibidas ou ocultadas (*esta configuração demonstra apenas se a opção Reparo automático da Proteção Residente está ativada*).

- ***Exibir notificações da bandeja sobre verificação*** *(ativada por padrão)* - decida se devem ser exibidas as informações sobre o início automático da verificação agendada, seu andamento e resultados.

- ***Exibir notificações da bandeja do Firewall*** *(ativado por padrão)* - decida se as informações relativas ao status e aos processos do Firewall, como avisos de ativação/desativação do componente, possível bloqueio de tráfego etc. devem ser exibidas. Este item fornece mais duas opções específicas de seleção *(para obter explicações detalhadas de cada um, consulte o capítulo Firewall deste documento)*:

  - ***Exibir notificações sobre alterações de perfil*** *(ativada por padrão)* - notifica você sobre mudanças automáticas de perfis do Firewall.

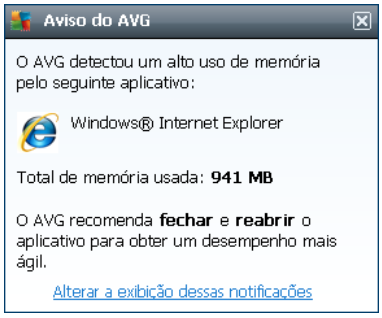
  - ***Exibir notificações sobre novas regras de aplicativo criadas*** *(desativada por padrão)* - notifica sobre a criação automática de regras do Firewall para novos aplicativos, com base em uma lista segura.

- ***Exibir notificações da bandeja relacionadas ao Verificador de E-mail*** *(ativada por padrão)* - decida se as informações sobre a verificação de todas as mensagens de e-mail de entrada e saída devem ser exibidas.

- ***Exibir notificações estatísticas*** *(ativada por padrão)* - mantenha a opção selecionada para permitir que notificações regulares de análises estatísticas sejam exibidas na bandeja do sistema.

- ***Exibir notificações da bandeja sobre o AVG Accelerator*** *(ativada por padrão)* - decida se devem ser exibidas informações sobre as atividades do ***AVG Accelerator***. O serviço ***AVG Accelerator***, que permite uma reprodução melhor de vídeos online e facilita downloads adicionais.

- ***Exibir notificações sobre o desempenho do AVG Advice*** *(ativada por padrão)* - o ***AVG Advice*** monitora o desempenho de navegadores da Internet suportados *(Internet Explorer, Chrome, Firefox, Opera e Safari)* e informa você caso um navegador exceda o uso do volume de memória recomendado. Nessa situação, o desempenho do computador poderá ser reduzido significativamente, e recomenda-se que o navegador da Internet seja reiniciado para acelerar os processos. Deixe ativado o item ***Exibir notificações sobre o desempenho do AVG Advice*** para manter-se informado.

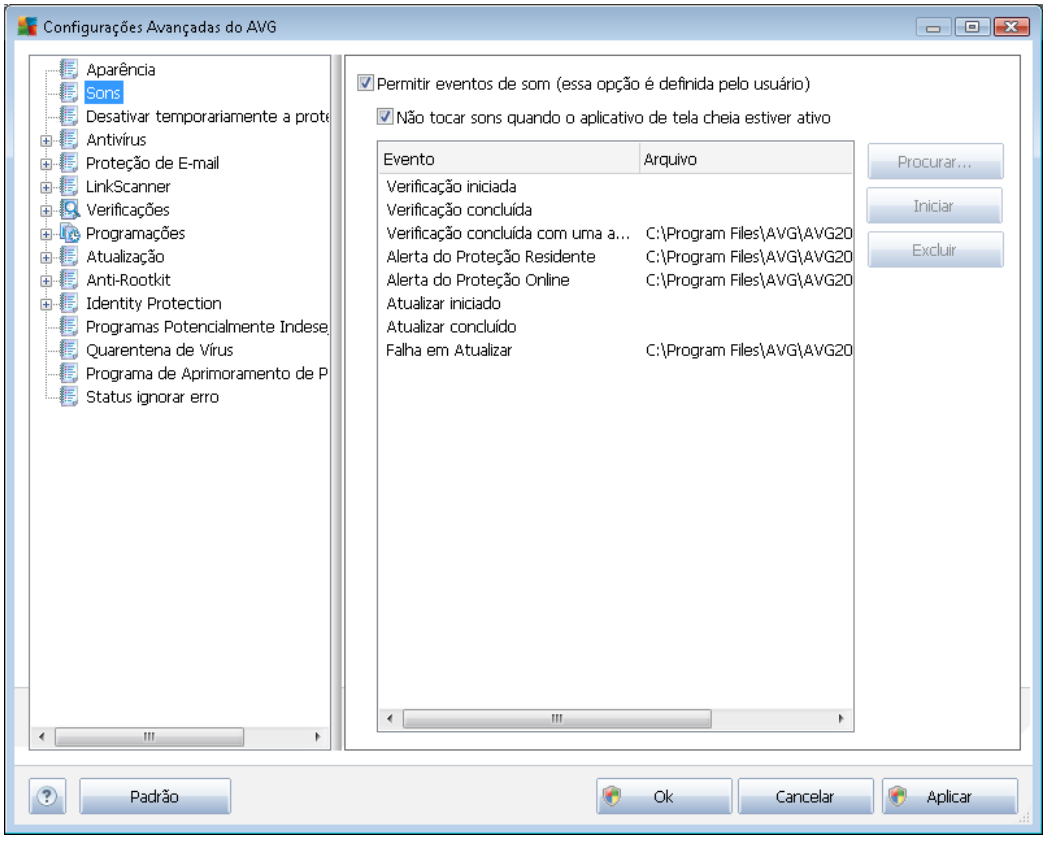


Modo de jogo

Esta função do AVG foi desenvolvida para aplicativos de tela inteira em que possíveis balões de informação do AVG (*exibidos, por exemplo, quando uma verificação programada é iniciada*) poderiam gerar problemas (*podem minimizar o aplicativo ou corromper seus gráficos*). Para evitar essa situação, mantenha marcada a caixa de seleção referente à opção ***Ativar modo de jogo quando um aplicativo de tela inteira for executado*** (*configuração padrão*).

9.2. Sons

Na caixa de diálogo ***Sons***, é possível especificar se deseja receber informações sobre ações especificas do **AVG Internet Security 2012** por meio de uma notificação sonora:



As configurações são válidas somente para o usuário de conta atual, ou seja, cada usuário do computador pode ter suas próprias configurações de som. Para permitir a notificação sonora, mantenha a opção ***Permitir eventos de som*** marcada (*a opção está ativada por padrão*) para ativar a lista de todas as ações relevantes. Além disso, você também pode marcar a opção ***Não tocar sons quando aplicativo de tela cheia estiver ativo*** para desativar a notificação sonora em situações em que ela pode ser disruptiva *(consulte também a seção Modo de jogo, no capítulo Configurações avançadas/Aparência neste documento)*.

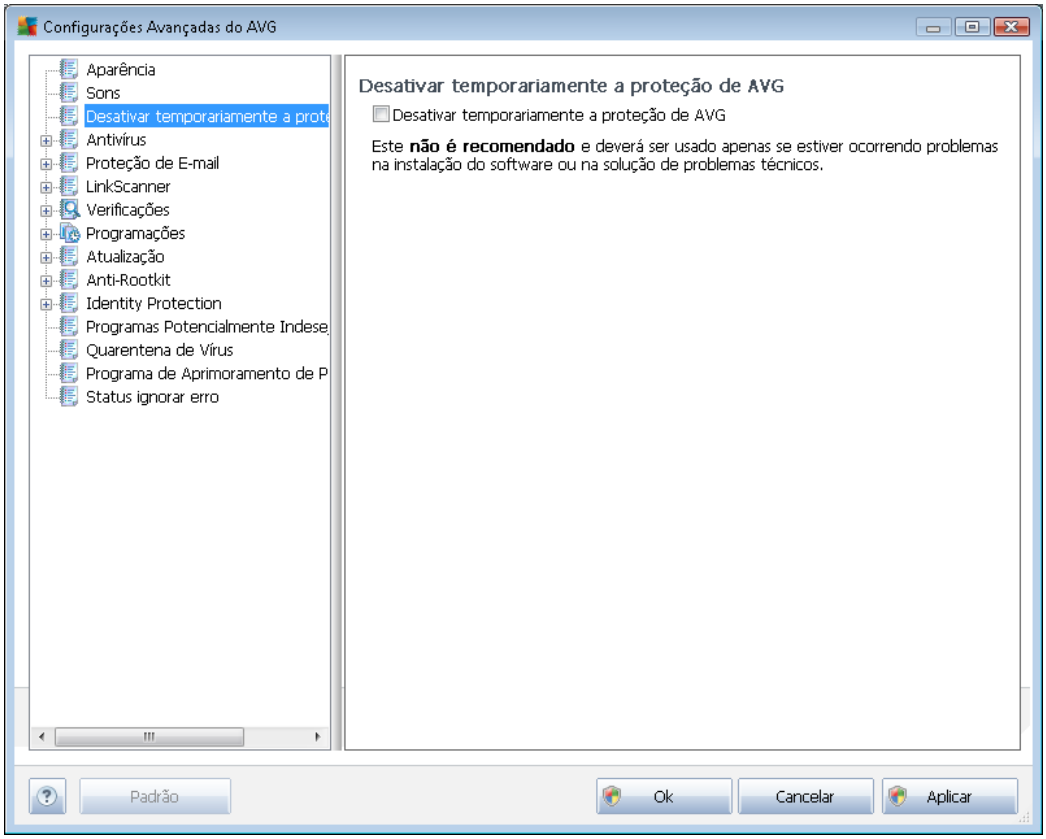
Botões de controle

- ***Procurar*** - com o evento respectivo selecionado na lista, use o botão ***Procurar*** para localizar e atribuir o arquivo de som desejado no seu disco. *(Somente sons no formato *.wav são suportados no momento.)*
- ***Iniciar*** - para ouvir o som selecionado, realce o evento na lista e pressione o botão ***Iniciar***.
- ***Excluir*** - use o botão ***Excluir*** para remover o som atribuído a um evento específico.

9.3. Desativar temporariamente a proteção do AVG

Na caixa de diálogo ***Desativar temporariamente a proteção do AVG***, você tem a opção de desativar toda a proteção oferecida pelo **AVG Internet Security 2012** de uma vez.

Lembre-se de que você não deve usar essa opção, a menos que ela seja absolutamente necessária!

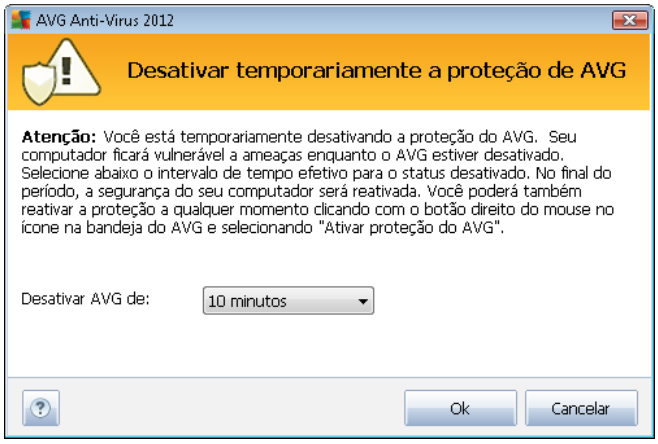


Na maioria dos casos, ***não é necessário*** desativar o **AVG Internet Security 2012** antes de instalar novo software ou novos drivers, nem mesmo se o instalador ou assistente de software sugerir que programas e aplicativos em execução devem ser encerrados primeiro para garantir que não haja interrupções indesejadas durante o processo de instalação. Caso você tenha algum problema durante a instalação, tente desativar a proteção residente (*Habilitar Proteção Residente*) primeiro. Se for necessário desativar temporariamente o **AVG Internet Security 2012**, você deverá reativá-lo assim que concluir a tarefa que solicitou a desativação. Se você estiver conectado à Internet ou a uma rede durante o período em que o software antivírus está desativado, o computador ficará vulnerável a ataques.

Como desativar a proteção do AVG

- Marque a caixa de seleção ***Desativar temporariamente a proteção AVG*** e confirme sua opção, pressionando o botão ***Aplicar***.

- Na caixa de diálogo recém-aberta, ***Desativar temporariamente a proteção AVG***, especifique por quanto tempo você deseja manter o **AVG Internet Security 2012** desativado. Por padrão, a proteção ficará desativada por 10 minutos, o que deve ser suficiente para qualquer tarefa comum, como instalação de novo software etc. O limite de tempo inicial é de 15 minutos e não pode ser substituído por outro valor por motivos de segurança. Após o período especificado, todos os componentes desativados serão automaticamente reativados.

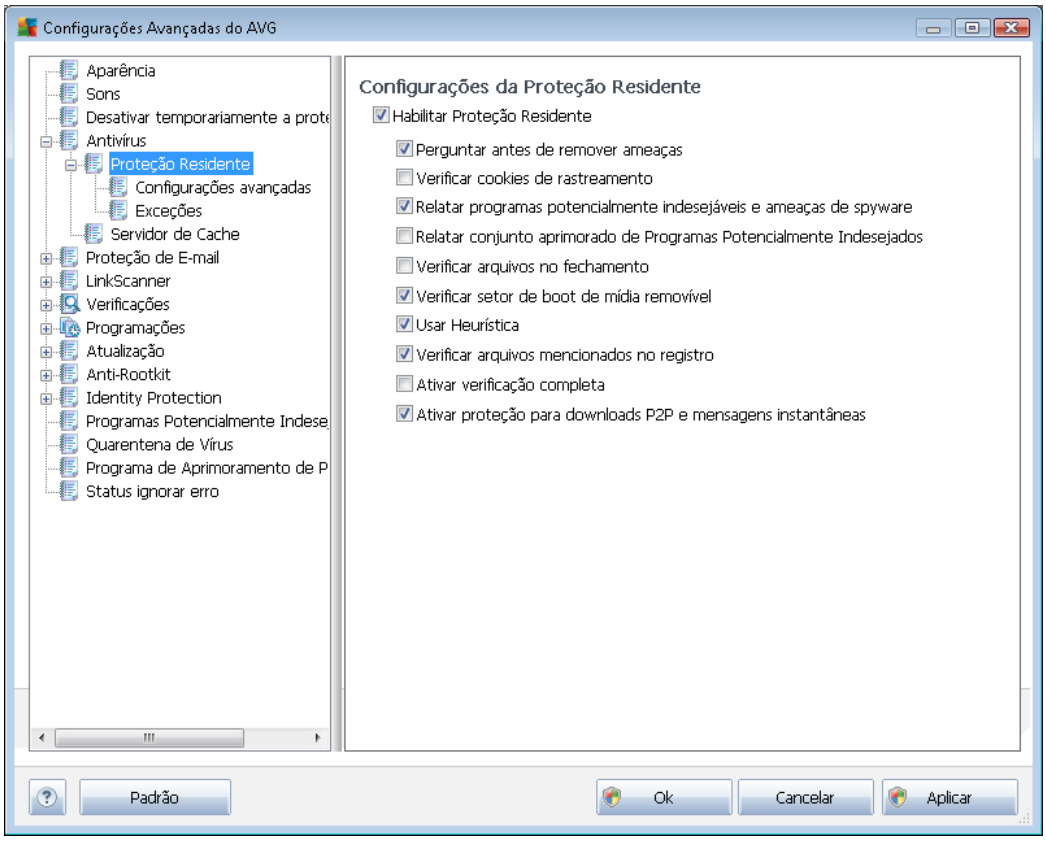


9.4. Antivírus

Inserir texto principal aqui.

9.4.1. Proteção Residente

A Proteção Residente realiza a proteção ao vivo contra vírus, spywares e outros malwares em arquivos e pastas.



Na caixa de diálogo ***Configurações da Proteção Residente*** , é possível ativar ou desativar a

Proteção Residente completamente marcando/desmarcando o item ***Ativar Proteção Residente*** (*essa opção é ativada por padrão*). Além disso, você pode selecionar os recursos da proteção residente que devem ser ativados:

- ***Verificar cookies de rastreamento*** (*desativado por padrão*) - este parâmetro define que os cookies devem ser detectados durante a verificação. (*Cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de site ou o conteúdo de suas compras eletrônicas.*)

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativado por padrão*) - marque para ativar o mecanismo Anti-Spyware e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativado por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão em perfeito estado e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar arquivos no fechamento*** (*desativado por padrão*) - a verificação durante o fechamento garante que o AVG examine objetos ativos (por exemplo, aplicativos, documentos etc.) quando forem abertos e também quando forem fechados. Este recurso ajuda a proteger o computador contra alguns tipos de vírus sofisticados.

- ***Verificar setor de inicialização de mídia removível*** (*ativada por padrão*)

- ***Usar Heurística*** (*ativado por padrão*) - a análise heurística será usada para detecção (*emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual*).

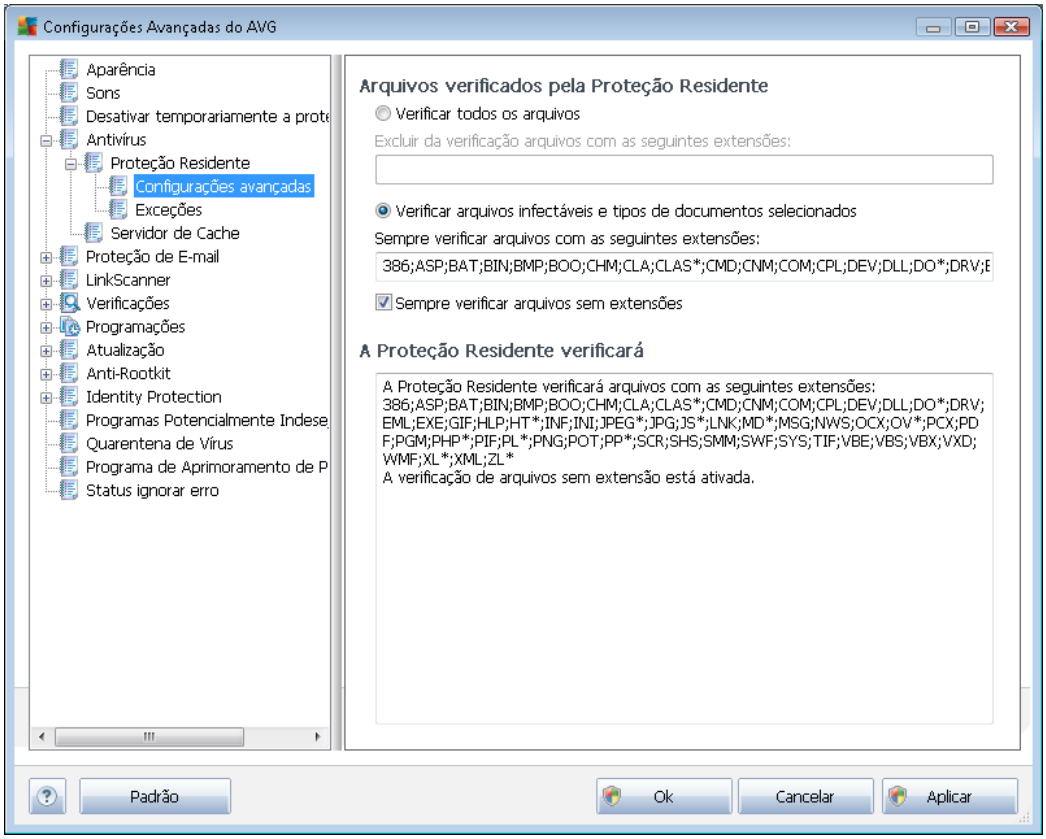
- ***Remover todas as ameaças automaticamente*** (*desativado por padrão*) - se houver solução disponível, qualquer infecção detectada será reparada automaticamente, e todas as infecções que não puderem ser solucionadas serão removidas.

- ***Verificar arquivos mencionados no registro*** (*ativado por padrão*) - este parâmetro define que o AVG verificará todos os arquivos executáveis adicionados ao registro de inicialização para evitar que uma infecção conhecida seja executada na próxima inicialização do computador.

- ***Ativar verificação completa*** (*desativado por padrão*) - em situações específicas (*como um estado de extrema emergência*), você pode marcar esta opção para ativar os algoritmos mais completos, que examinarão todos os objetos de ameaça possíveis minuciosamente. Entretanto, lembre-se de que esse método consome bastante tempo.

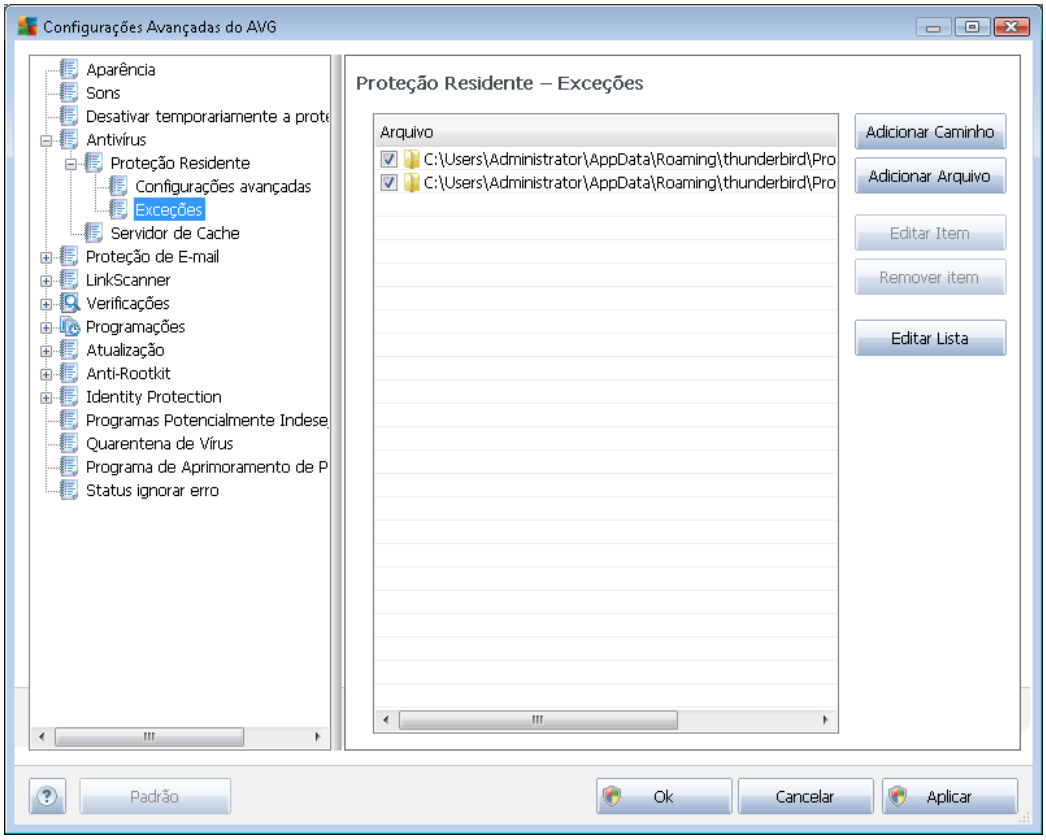
- ***Ativar a proteção para mensagens instantâneas e download P2P*** (*ativado por padrão*) - marque este item para verificar se há vírus em comunicações por mensagens instantâneas (*como ICQ, MSN Messenger etc.*) e em downloads P2P.

Na caixa de diálogo ***Arquivos verificados pela Proteção Residente***, é possível configurar os arquivos que serão verificados (*por extensão específica*):



Marque a caixa de seleção respectiva para decidir se deseja ***Verificar todos os arquivos*** ou ***Verificar arquivos infectáveis e tipos de documentos selecionados*** somente. Se você optou pela segunda opção, poderá especificar uma lista de extensões definindo os arquivos que devem ser excluídos da verificação, além de especificar uma lista de extensões de arquivos que definem os arquivos que devem ser verificados sob todas as circunstâncias.

A seção abaixo denominada ***Proteção Residente vai verificar*** sintetiza as configurações atuais, exibindo uma visão geral detalhada do que a ***Proteção Residente*** irá realmente verificar.



A caixa de diálogo ***Proteção Residente - Exceções*** oferece a possibilidade de definir as pastas e/ou os arquivos que devem ser excluídos da verificação da ***Proteção Residente***.

Se isso não for necessário, é altamente recomendável não excluir nenhum item.

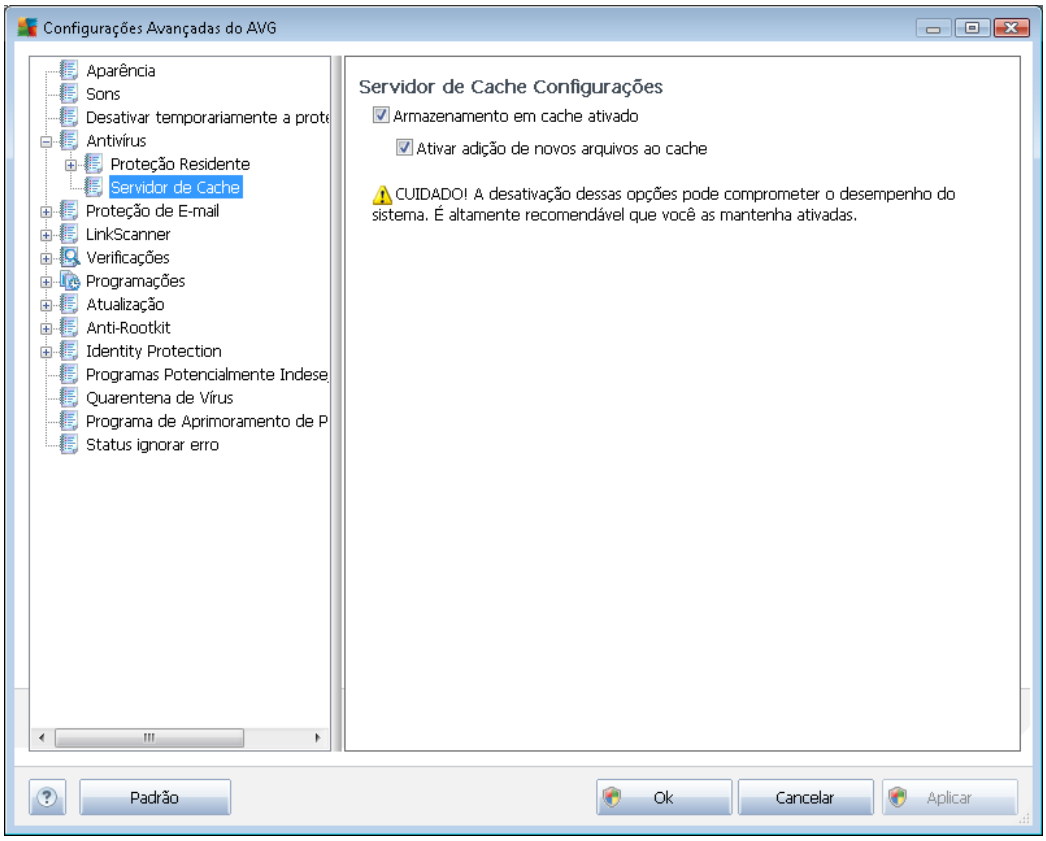
Botões de controle

Essa caixa de diálogo fornece os seguintes botões de controle:

- ***Adicionar Caminho*** – especifique um diretório (diretórios) a ser excluído da verificação, selecionando-o (um a um, no caso de haver mais de um) na árvore de navegação do disco local
- ***Adicionar Arquivo*** – especifique arquivos a serem excluídos da verificação, selecionando-os um a um na árvore de navegação do disco local
- ***Editar Item*** – permite editar o caminho especificado para um arquivo ou pasta selecionado
- ***Remover Item*** – permite excluir o caminho para um item selecionado da lista
- ***Editar Lista*** - permite editar a lista completa de exceções definidas em uma nova caixa de diálogo que se comporta como um editor de texto padrão

9.4.2. Servidor de cache

A caixa de diálogo ***Configurações do servidor de cache*** se refere ao processo do servidor de cache desenvolvido para agilizar todos os tipos de verificações do **AVG Internet Security 2012**:



O servidor de cache coleta e mantém informações de arquivos confiáveis (*um arquivo é considerado confiável se tiver a assinatura digital de uma fonte confiável*). Esses arquivos são automaticamente identificados como sendo seguros e não precisam ser verificados novamente. Portanto, eles são ignorados durante a verificação.

A caixa de diálogo ***Configurações do servidor de cache*** oferece as seguintes opções de configuração:

- ***Caching ativado*** (*ativado por padrão*) - desmarque a caixa para desativar o***Servidor de Cache*** e esvaziar a memória de cache. Observe que a verificação pode desacelerar, e o desempenho global de computador diminuir, conforme é feita a verificação de todos os arquivos únicos em uso procurando primeiro pela existência de vírus e spyware.

- ***Ativar inclusão de novos arquivos em cache*** (*ativado por padrão*) - desmarque a caixa para parar de adicionar mais arquivos na memória cache. Todos os arquivos já armazenados em cache serão mantidos e utilizados até que o cache seja desativado completamente, ou até a próxima atualização do banco de dados de vírus.

A menos que você tenha um bom motivo para desativar o servidor de cache, recomendamos manter as configurações padrão e deixar a opção ativada. Caso contrário, você poderá sentir

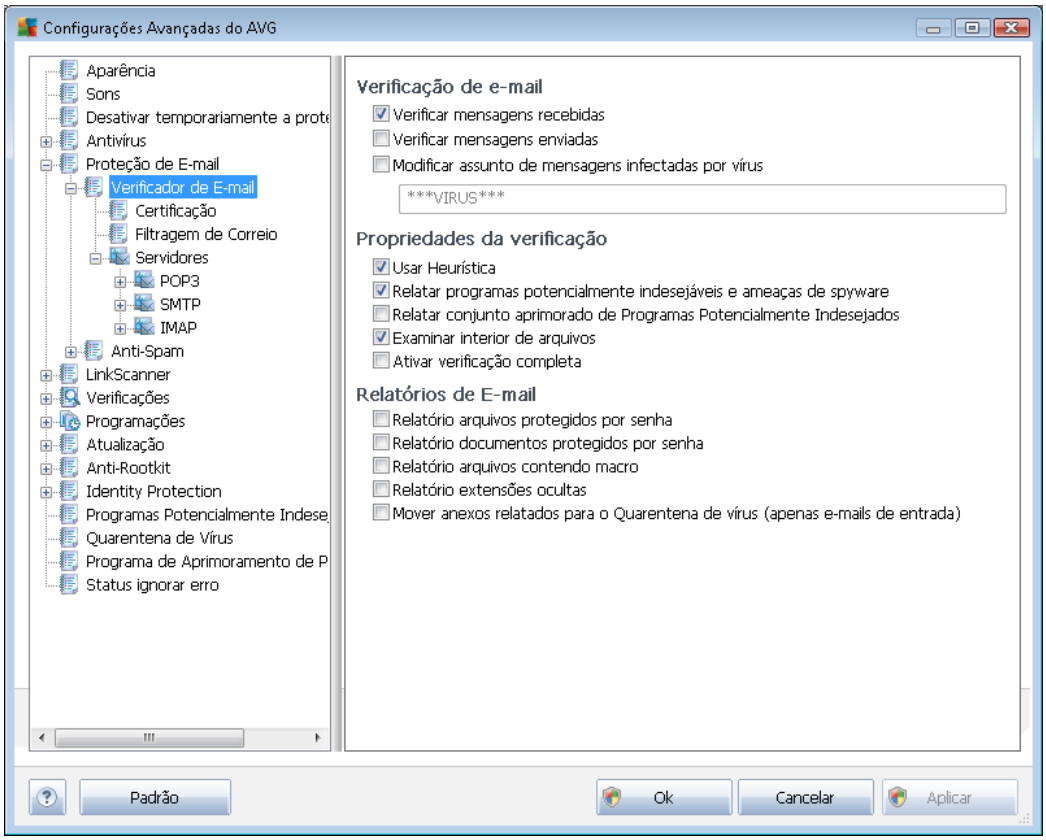
uma redução significativa na velocidade e no desempenho de seu sistema.

9.5. Proteção de e-mail

Na seção ***Proteção de e-mail***, é possível editar configurações detalhadas do Verificador de E-mail e do Anti-Spam:

9.5.1. Verificador de e-mail

A caixa de diálogo ***Verificador de E-mail*** é dividida em três seções:



Verificação de e-mail

Nesta seção, você pode definir as funções básicas a seguir para mensagens de e-mail recebidas e/ou enviadas:

- ***Verificar mensagens recebidas*** (*ativada por padrão*) - marque para ativar/desativar a opção de verificação de todas as mensagens de email enviadas ao seu cliente de email
- ***Verificar mensagens enviadas*** (*desativada por padrão*) - marque para ativar/desativar a opção de verificação de todos os emails enviados de sua conta
- ***Modificar assunto de mensagens infectadas por vírus*** (*desativada por padrão*) - se quiser ser avisado de que a mensagem de email verificada foi considerada infecciosa, marque este item e digite o texto desejado no campo de texto. Esse texto será adicionado

ao campo "Assunto" para cada mensagem de e-mail detectada para facilitar a identificação e filtragem. O valor padrão recomendável é ***VIRUS***.

Propriedades da verificação

Nesta seção, você pode especificar como as mensagens de e-mail serão verificadas:

- ***Usar Heurística*** (*ativada por padrão*) - marque para usar o método de detecção de heurística ao verificar mensagens de e-mail. Quando essa opção está ativada, você pode filtrar anexos de e-mail não apenas por extensão, mas também o conteúdo real do anexo será considerado. A filtragem pode ser definida na caixa de diálogo Filtragem de e-mail.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo Anti-Spyware e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar dentro de arquivos*** (*ativada por padrão*) - marque para verificar os conteúdos de arquivos anexados às mensagens de e-mail.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*por exemplo, suspeita de que seu computador foi infectado por vírus ou invadido*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

Relatório de anexos de e-mail

Nesta seção, você pode definir relatórios adicionais sobre arquivos potencialmente perigosos ou suspeitos. Observe que nenhuma caixa de diálogo de advertência será exibida, apenas um texto de certificação será adicionado ao final da mensagem de e-mail e todos esses relatórios serão listados na caixa de diálogo Detecção do Verificador de e-mail:

- ***Reportar arquivos protegidos por senha*** – arquivos (*ZIP, RAR etc.*) protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa de seleção para reportá-los como potencialmente perigosos.

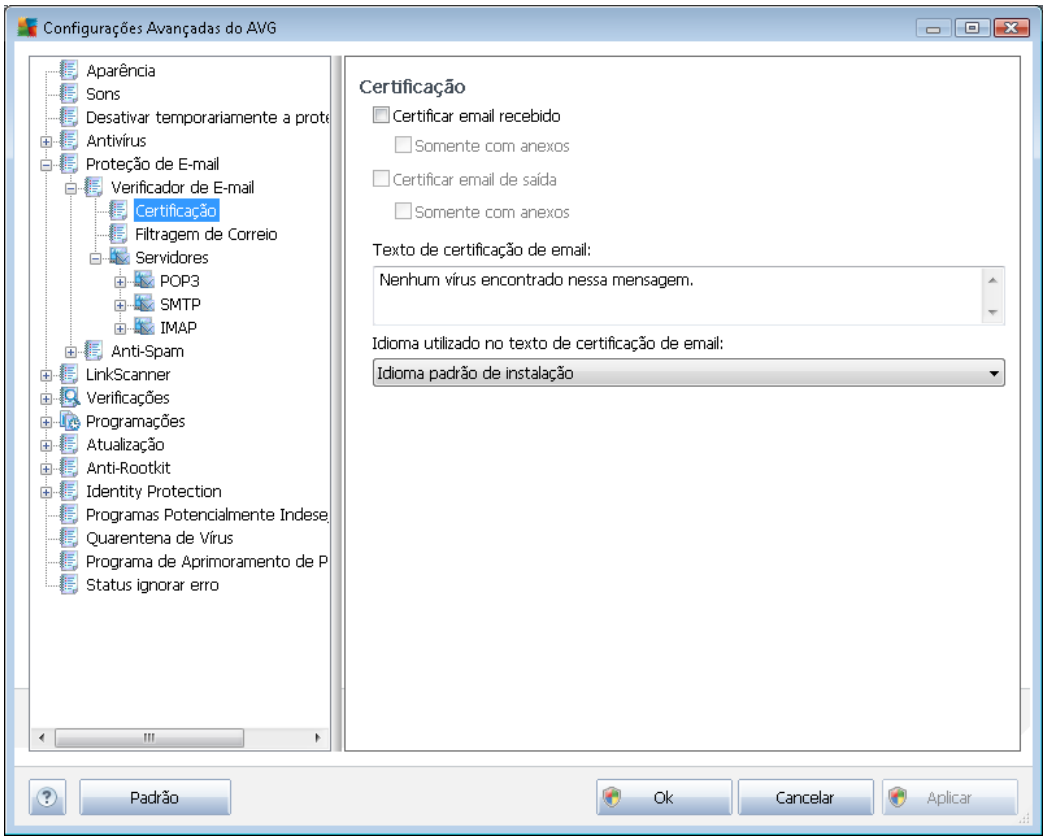
- ***Reportar documentos protegidos por senha*** – documentos protegidos por senha não podem ser verificados em busca de vírus. Marque a caixa de seleção para reportá-los como potencialmente perigosos.

- ***Reportar arquivos contendo macros*** – uma macro é uma sequência predefinida de etapas com o objetivo de executar certas tarefas mais fáceis para um usuário (*as macros do MS Word são amplamente conhecidas*). Dessa forma, uma macro pode conter instruções potencialmente perigosas e convém você marcar a caixa de seleção para garantir que os arquivos com macros sejam reportados como suspeitos.

- ***Reportar extensões ocultas –*** extensões ocultas podem fazer um arquivo executável suspeito, "alguma coisa.txt.exe", por exemplo, parecer-se com um arquivo de texto comum inofensivo "alguma coisa.txt". Marque a caixa de seleção para reportá-los como potencialmente perigosos.

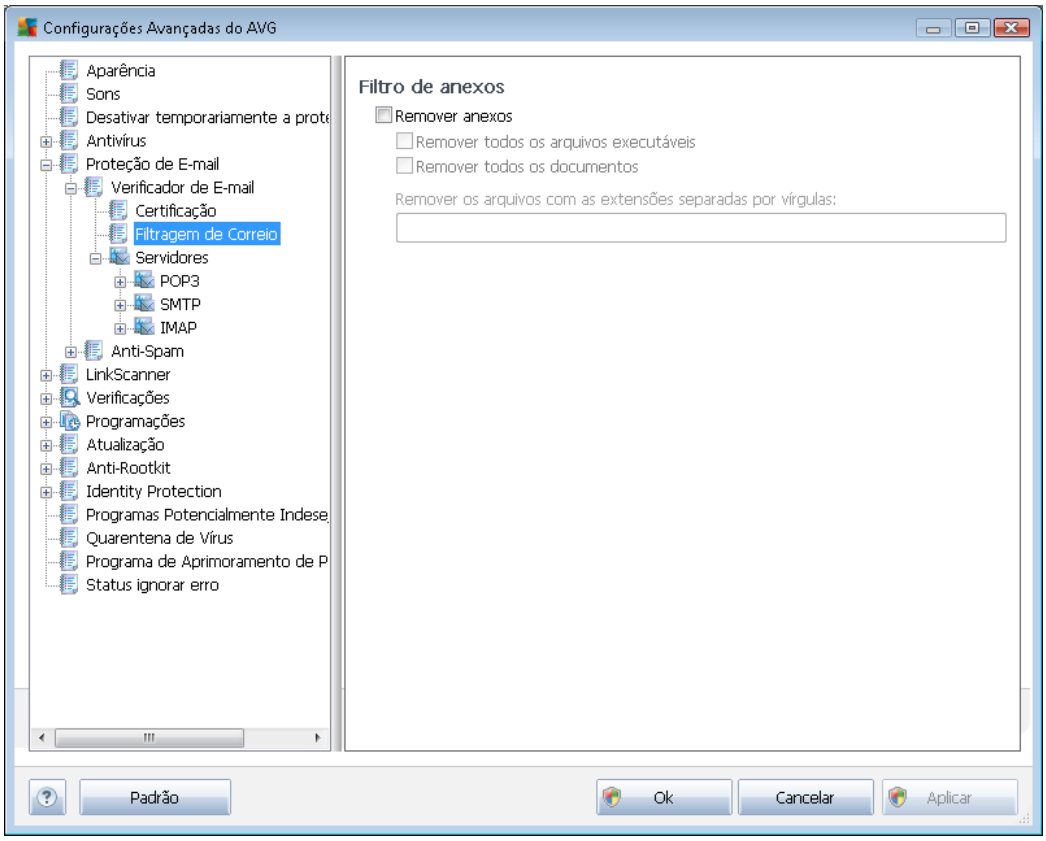
- ***Mover anexos de e-mail informados para a área de Quarentena*** - especifique se você deseja ser notificado por e-mail sobre arquivos protegidos por senha, documentos protegidos por senha, arquivos contendo macros e/ou arquivos com extensão oculta detectados como um anexo de uma mensagem de e-mail verificada. Se uma mensagem desse tipo for identificada durante a verificação, defina se o objeto infectado detectado deve ser movido para a Quarentena.

Na caixa de diálogo ***Certificação***, você pode selecionar as caixas específicas para decidir se deseja certificar e-mails recebidos (***Certificar e-mails recebidos***) e/ou e-mails enviados (***Certificar e-mails enviados***). Para cada uma dessas opções, você pode especificar o parâmetro ***Somente com anexos***, para que a certificação seja adicionada apenas às mensagens de e-mail com anexos:



Por padrão, o texto de certificação consiste em informações básicas com o aviso *Nenhum vírus encontrado nesta mensagem.* No entanto, essas informações podem ser estendidas ou alteradas conforme suas necessidades: escreva o texto de certificação desejado no campo ***Texto de certificação de e-mail***. Na seção ***Idioma utilizado no texto de certificação de e-mail***, você pode definir melhor em que idioma deve ser exibida a parte da certificação que é gerada automaticamente (*Nenhum vírus encontrado nesta mensagem*).

Observação: *somente o texto padrão será exibido no idioma solicitado, e o texto personalizado não será traduzido automaticamente.*



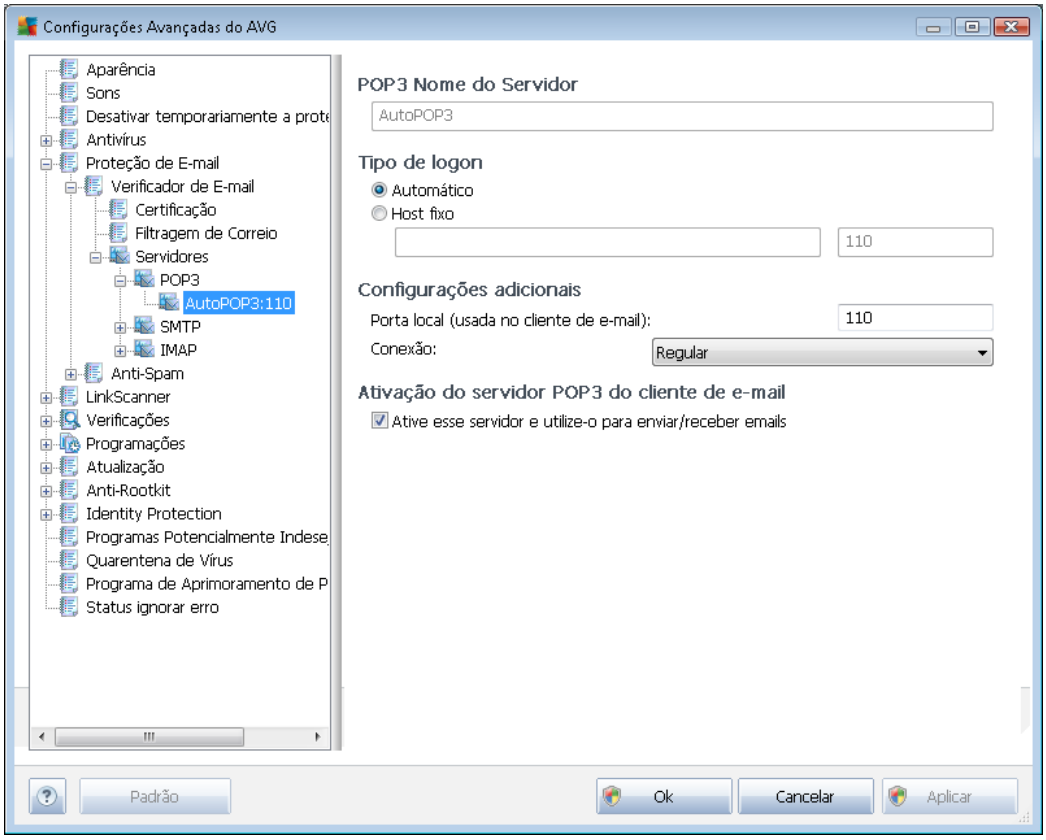
A caixa de diálogo ***Filtro de anexo*** permite configurar parâmetros para a verificação de anexos de mensagens de e-mail. Por padrão, a opção ***Remover anexos*** é desativada. Se você desejar ativá-la, todos anexos de mensagens de e-mail detectados como infectados ou potencialmente perigosos serão removidos automaticamente. Se você desejar especificar os tipos de anexo que devem ser removidos, selecione a opção apropriada:

- ***Remover todos os arquivos executáveis*** - todos os arquivos *.exe serão excluídos.
- ***Remover todos os documentos*** - todos os arquivos *.doc, *.docx, *.xls, *.xlsx serão excluídos.
- ***Remover arquivos com extensões separadas por vírgulas*** - removerá todos os arquivos com as extensões definidas.

Na seção ***Servidores***, você pode editar parâmetros dos servidores do Verificador de E-mail:

- Servidor POP3
- Servidor SMTP
- Servidor IMAP

Além disso, você também pode definir um novo servidor para e-mails de entrada e de saída usando o botão ***Adicionar novo servidor***.



Nessa caixa de diálogo (*aberta via* ***Servidores/POP3***), você pode configurar um novo servidor do Verificador de E-mail usando o protocolo POP3 para e-mails recebidos:

- ***Nome do Servidor POP3*** - neste campo, é possível especificar o nome dos servidores recém-adicionados (*para adicionar um servidor POP3, clique com o botão direito do mouse sobre o item POP3 do menu de navegação esquerdo*). Para o servidor "AutoPOP3" criado automaticamente, este campo fica desativado.
- ***Tipo de login*** - define o método para determinar o servidor de e-mail usado para e-mails recebidos:

- ***Automático*** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail.

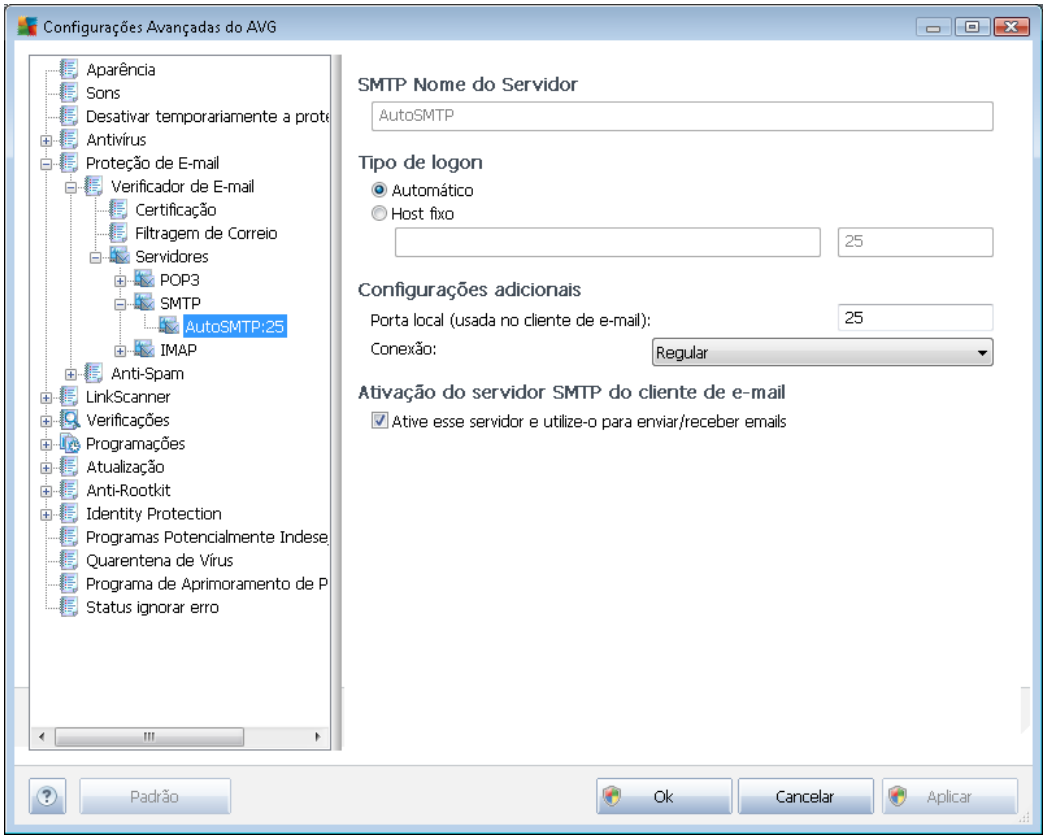
- ***Host fixo*** - Nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mail. O nome de login permanecerá inalterado. Para um nome, você pode usar um nome de domínio (*por exemplo, pop.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*). Se o servidor de e-mail usar uma porta não padrão, você poderá especificar essa porta depois do nome do servidor usando um ponto-e-vírgula como delimitador (*por exemplo, pop.acme.com:8200*). A porta padrão para a comunicação POP3 é 110.

- ***Configurações adicionais*** - especifica parâmetros mais detalhados:

  - ***Porta local*** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação POP3.

  - ***Conexão*** - no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso estará disponível somente quando houver suporte no servidor de e-mail de destino.

- ***Ativação do servidor POP3 do cliente de e-mail*** - marque/desmarque esse item para ativar ou desativar o servidor POP3 especificado



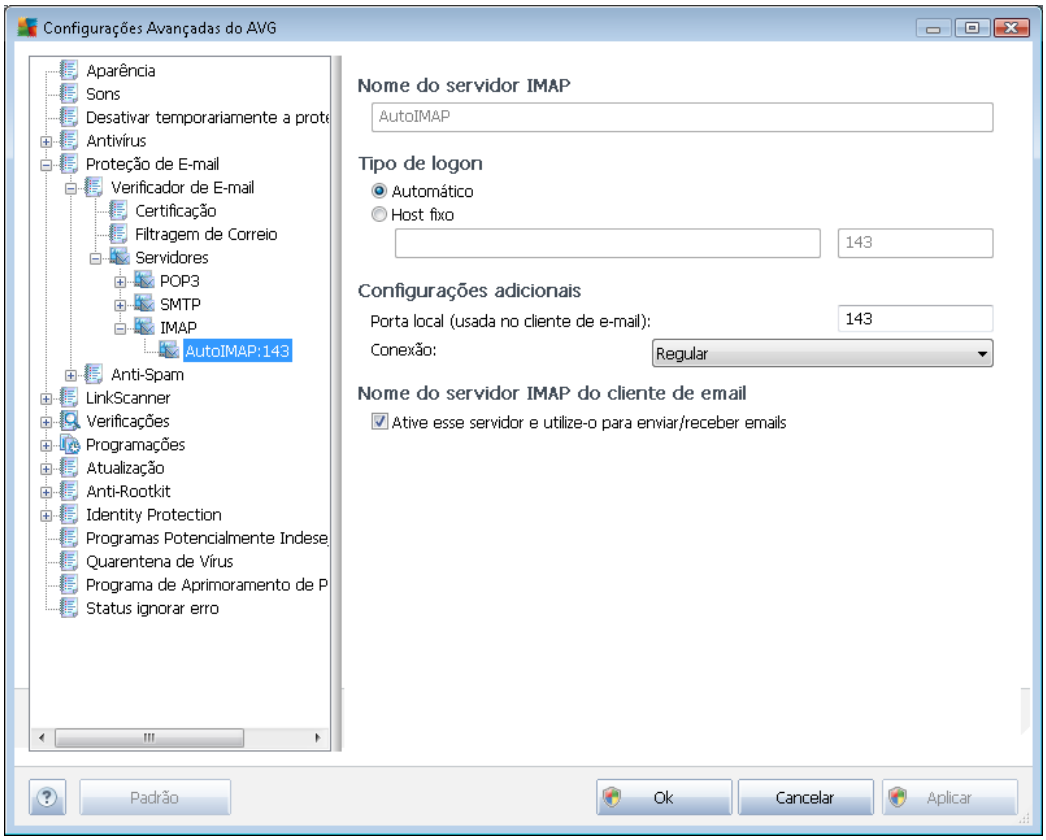
Nessa caixa de diálogo (*aberta via **Servidores/SMTP***), você pode configurar um novo servidor do Verificador de E-mail usando o protocolo SMTP para mensagens enviadas:

- ***Nome do Servidor SMTP*** - neste campo, é possível especificar o nome dos servidores recém-adicionados (*para adicionar um servidor SMTP, clique com o botão direito do mouse sobre o item SMTP do menu de navegação esquerdo*). Para o servidor "AutoSMTP" criado automaticamente, este campo fica desativado.
- ***Tipo de login*** - define o método para determinar o servidor de e-mail usado para e-mails enviados:
  - ***Automático*** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail
  - ***Host fixo*** - nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mails. Você pode usar um nome de domínio (*por exemplo, smtp.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de e-mail usar uma porta não padrão, você poderá digitar essa porta depois do nome do servidor usando dois pontos como delimitador (*por exemplo, smtp.acme.com:8200*). A porta padrão para a comunicação SMTP 25 é.
- ***Configurações adicionais*** - especifica parâmetros mais detalhados:

- ***Porta local*** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação SMTP.

- ***Conexão*** - no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso está disponível somente quando houver suporte no servidor de e-mail de destino.

- ***Ativação do servidor SMTP do cliente de e-mail*** - marque/desmarque esse item para ativar ou desativar o servidor SMTP especificado



Nessa caixa de diálogo (aberta via ***Servidores/IMAP***), você pode configurar um novo servidor do Verificador de E-mail usando o protocolo IMAP para mensagens enviadas:

- ***Nome do Servidor IMAP*** - neste campo, é possível especificar o nome dos servidores recém-adicionados (*para adicionar um servidor IMAP, clique com o botão direito do mouse sobre o item IMAP do menu de navegação esquerdo*). Para o servidor "AutoIMAP" criado automaticamente, este campo fica desativado.

- ***Tipo de login*** - define o método para determinar o servidor de e-mail usado para e-mails enviados:

- ***Automático*** - o login será feito automaticamente, de acordo com as configurações do cliente de e-mail

- ***Host fixo*** - nesse caso, o programa sempre usará o servidor especificado aqui. Especifique o endereço ou nome do servidor de e-mails. Você pode usar um nome de domínio (*por exemplo, smtp.acme.com*) assim como um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de e-mail usar uma porta não padrão, você poderá digitar essa porta depois do nome do servidor usando dois pontos como delimitador (*por exemplo, imap.acme.com:8200*). A porta padrão para a comunicação IMAP é 143.

- ***Configurações adicionais*** - especifica parâmetros mais detalhados:

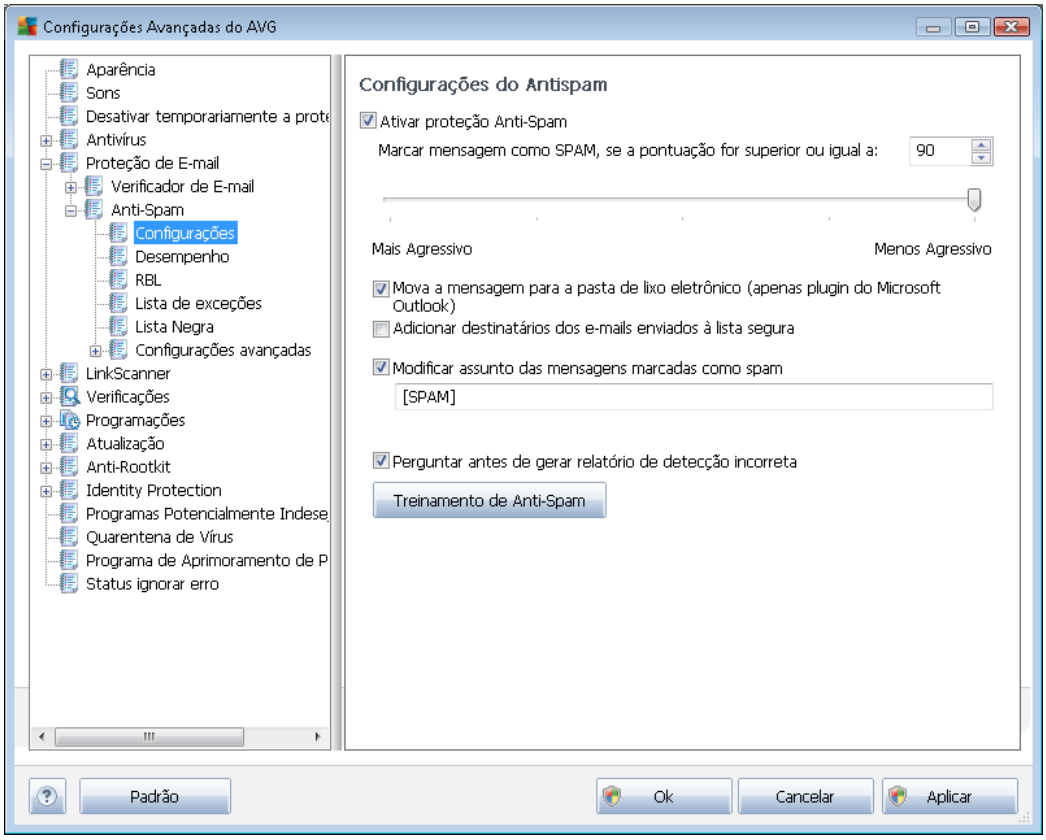
  - ***Porta local*** - especifica a porta em que a comunicação do seu aplicativo de e-mail deverá ser esperada. Em seguida, você deve especificar esta porta no aplicativo de e-mail como a porta para comunicação IMAP

  - ***Conexão*** - no menu suspenso, é possível especificar o tipo de conexão que será usada (*regular/SSL/SSL padrão*). Se você escolher a conexão SSL, os dados enviados serão criptografados sem o risco de controle ou monitoramento de terceiros. Esse recurso está disponível somente quando houver suporte no servidor de e-mail de destino.

- ***Ativação do servidor IMAP do cliente de e-mail*** - marque/desmarque este item para ativar ou desativar o servidor IMAP especificado acima

9.5.2. Anti-Spam

Inserir texto principal aqui.



Na caixa de diálogo ***Configurações Anti-Spam***, é possível marcar/desmarcar a caixa de seleção ***Ativar proteção do Anti-Spam*** para permitir/proibir a verificação antispam em comunicações por e-mail. Essa opção está ativada por padrão e, como sempre, convém manter essa configuração, a não ser que você tenha um motivo concreto para alterá-la.

Em seguida, você também pode selecionar medidas de pontuação mais ou menos agressivas. O ***filtro Anti-Spam***atribui a cada mensagem uma pontuação (*ou seja, o nível de semelhança entre um SPAM e o conteúdo da mensagem*), com base em várias técnicas dinâmicas de verificação. É possível ajustar a configuração ***Marcar mensagem como spam se o resultado for superior a*** digitando o valor ou movendo o controle deslizante para a esquerda ou para a direita (*o intervalo dos valores é limitado a 50 a 90*).

Em geral, recomendamos a definição do limite entre 50 e 90 ou, em caso de dúvidas, como 90. Veja uma análise geral do limite de pontuação:

- ***Valor entre 80 e 90*** - As mensagens de e-mail que parecem ser spam serão filtradas. Algumas mensagens que não são SPAM poderão ser bloqueadas incorretamente.
- ***Valor entre 60 e 79*** - uma configuração considerada bastante agressiva. As mensagens de e-mail que provavelmente são spam serão filtradas. É provável que mensagens não spam também sejam bloqueadas
- ***Valor entre 50 e 59*** - Configuração muito agressiva. É provável que mensagens de e-mail

não spam sejam bloqueadas como verdadeiras mensagens spam. Esse intervalo limite não é recomendado para uso normal.

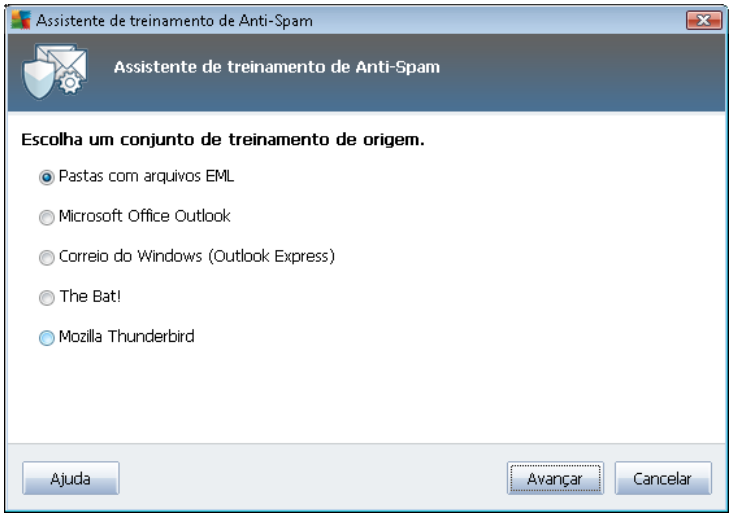
Na caixa de diálogo ***Configurações Anti-Spam***, você pode definir melhor como as mensagens de e-mail de spam detectadas devem ser tratadas:

- ***Mover mensagens para a pasta Lixo*** - marque essa caixa de seleção para especificar se cada mensagem de spam deve ser automaticamente movida para a pasta de lixo específica dentro do cliente de e-mail;
- ***Adicionar destinatários de e-mails enviados à lista de exceções*** - marque essa caixa de seleção para confirmar que todos os destinatários de e-mails enviados são confiáveis e que todas as mensagens de e-mail provenientes das contas desses destinatários podem ser entregues;
- ***Modificar assunto das mensagens marcadas como vírus*** - marque essa caixa de seleção se quiser que todas as mensagens detectadas como spam sejam marcadas com uma palavra ou um caractere específico no campo de assunto do e-mail. O texto desejado pode ser digitado no campo de texto ativado.
- ***Perguntar antes de gerar relatório de detecção incorreta*** - contanto que, durante o processo de instalação, você tenha concordado em participar do Programa de Aprimoramento de Produto. Se for o caso, você autoriza a geração de relatório de ameaças detectadas para a AVG. A geração de relatório é feita automaticamente. Entretanto, você pode marcar esta caixa de seleção para configurar que deseja que uma pergunta seja feita antes de relatar qualquer spam detectado à AVG, para ter certeza de que a mensagem deva realmente ser classificada como spam.

Botões de controle

Botão Treinamento Anti-Spam abre o Assistente de treinamento Anti-Spam descrito de maneira detalhada no próximo capítulo.

A primeira caixa de diálogo do ***Assistente de treinamento de anti-spam*** solicita que você selecione a origem das mensagens de e-mail que deseja usar para treinamento. Normalmente, convém usar e-mails marcados incorretamente como SPAM ou mensagens de spam que não foram reconhecidas.



Existem as seguintes opções dentre as quais escolher:

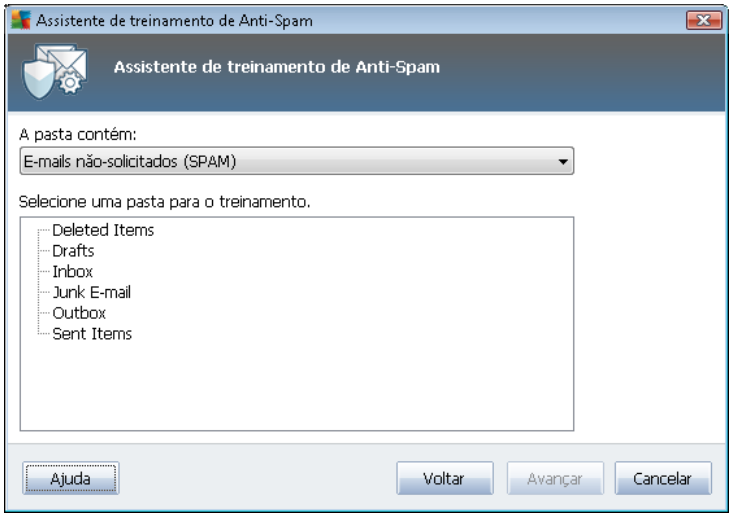
- ***Um cliente de e-mail específico*** - se você usa um dos clientes de e-mail listados (*MS Outlook, Outlook Express, The Bat!*), basta selecionar a opção correspondente
- ***Pasta com arquivos EML*** - se você usa qualquer outro programa de e-mail, salve primeiro as mensagens em uma pasta específica (*no formato .eml*) ou certifique-se de que conhece o local das pastas de mensagens do cliente de e-mail. Em seguida, selecione ***Pasta com arquivos EML***, o que permitirá que você localize a pasta desejada na próxima etapa

Para um processo de treinamento mais rápido e fácil, é uma boa idéia organizar os e-mails nas pastas antecipadamente, para que a pasta que você usará para treinamento contenha apenas as mensagens de treinamento (desejadas ou indesejadas). Entretanto, isso não é necessário, uma vez que você poderá filtrar os e-mails posteriormente.

Selecione a opção apropriada e clique em ***Avançar*** para continuar com o assistente.

A caixa de diálogo exibida nesta etapa depende da seleção anterior.

Pastas com arquivos EML



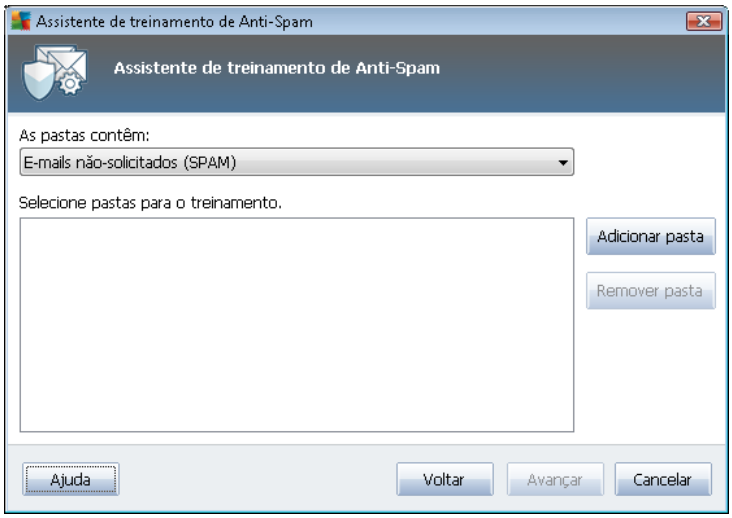
Nesta caixa de diálogo, selecione a pasta com as mensagens que deseja usar para treinamento. Pressione o botão ***Adicionar pasta*** para localizar a pasta com os arquivos .eml (*mensagens de e-mail salvas*). A pasta selecionada será então exibida na caixa de diálogo.

No menu suspenso ***As pastas contêm***, defina uma das duas opções - se a pasta selecionada deve conter mensagens desejadas (*HAM*) ou mensagens não solicitadas (*SPAM*). Lembre-se de que você poderá filtrar as mensagens na próxima etapa, de modo que a pasta não precisa conter somente e-mails de treinamento. Você pode também remover as pastas selecionadas não desejadas da lista clicando no botão ***Remover pasta***.

Quando terminar, clique em ***Avançar*** e passe para Opções de filtragem de mensagem.

Cliente de e-mail específico

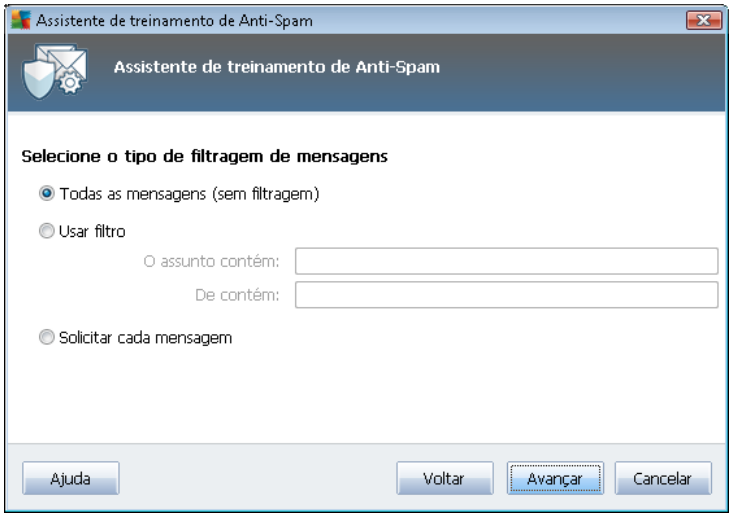
Após confirmar uma das opções, será exibida uma nova caixa de diálogo.



Observação: *no caso do Microsoft Office Outlook, será necessário selecionar o perfil do MS Office Outlook primeiro.*

No menu suspenso ***As pastas contêm***, defina uma das duas opções - se a pasta selecionada deve conter mensagens desejadas (*HAM*) ou mensagens não solicitadas (*SPAM*). Lembre-se de que você poderá filtrar as mensagens na próxima etapa, de modo que a pasta não precisa conter somente e-mails de treinamento. Uma árvore de navegação do cliente de e-mail selecionado já está exibida na seção principal da caixa de diálogo. Localize a pasta desejada na árvore e realce-a com o seu mouse.

Quando terminar, clique em ***Avançar*** e passe para Opções de filtragem de mensagem.



Nesta caixa de diálogo, você poderá definir a filtragem das mensagens de e-mail.

- ***Todas as mensagens (sem filtragem)*** - se você tiver certeza de que a pasta selecionada contém somente as mensagens que deseja usar no treinamento, selecione a opção ***Todas as mensagens (sem filtragem)***.

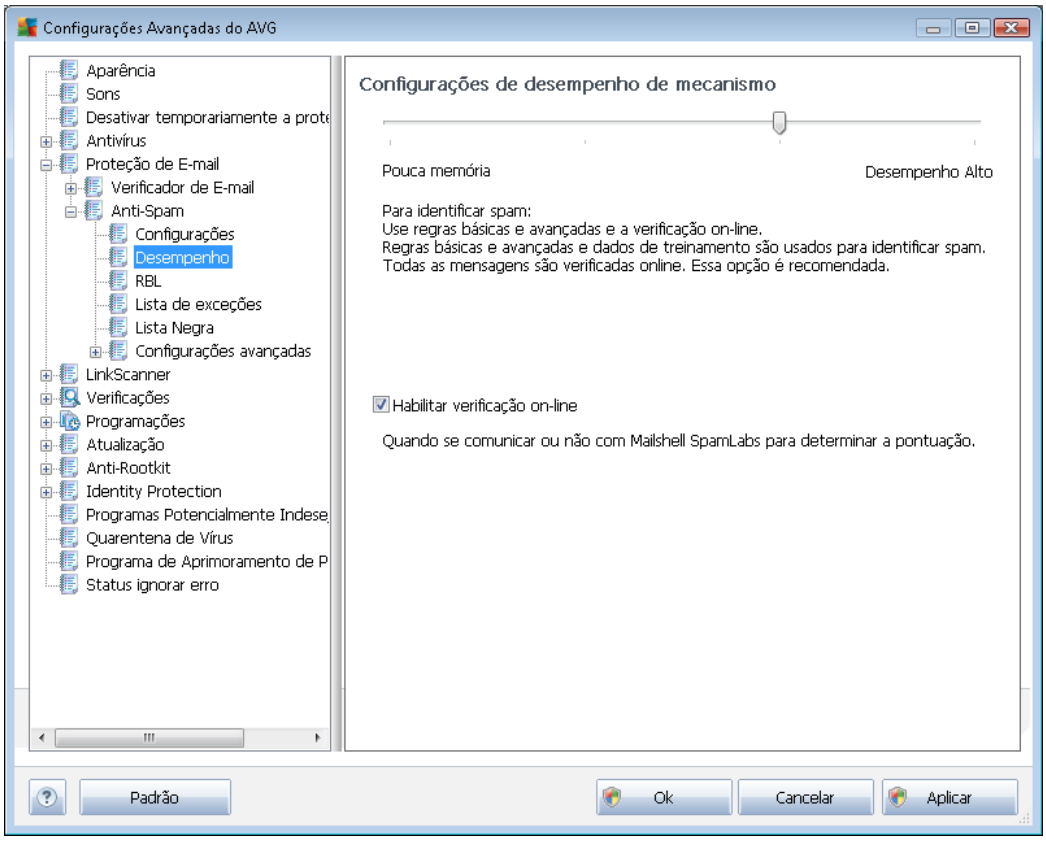
- ***Usar filtro*** - para obter uma filtragem mais avançada, selecione a opção ***Usar filtro***. Você pode inserir uma palavra *nome*), parte de uma palavra ou frase a ser pesquisada no assunto de e-mail e/ou no campo do remetente. Todas as mensagens que correspondem exatamente aos critérios inseridos serão usadas para o treinamento, sem solicitações adicionais. Quando você preenche ambos os campos de texto, os endereços que correspondem a apenas uma das duas condições serão usados também!

- ***Perguntar em cada mensagem*** - se você não estiver certo sobre as mensagens contidas na pasta e quiser que o assistente faça perguntas sobre cada mensagem *(para poder determinar se ela deve ser usada para treinamento ou não)*, selecione a opção ***Perguntar em cada mensagem***.

Quando a opção apropriada for selecionada, clique em ***Avançar***. A caixa de diálogo a seguir terá caráter apenas informativo, informando que o assistente está pronto para processar as mensagens. Para iniciar o treinamento, clique no botão ***Avançar*** novamente. O treinamento será iniciado de

acordo com as condições selecionadas previamente.

A caixa de diálogo ***Configurações de desempenho do mecanismo*** (*que pode ser acessada por meio do link no item* ***Desempenho*** *do painel de navegação esquerdo*) oferece as configurações de desempenho do componente ***Anti-Spam***.



Mova o controle deslizante para a esquerda ou para a direita para alterar o nível de intervalo de desempenho de verificação entre os modos ***Pouca memória***/***Alto desempenho***.

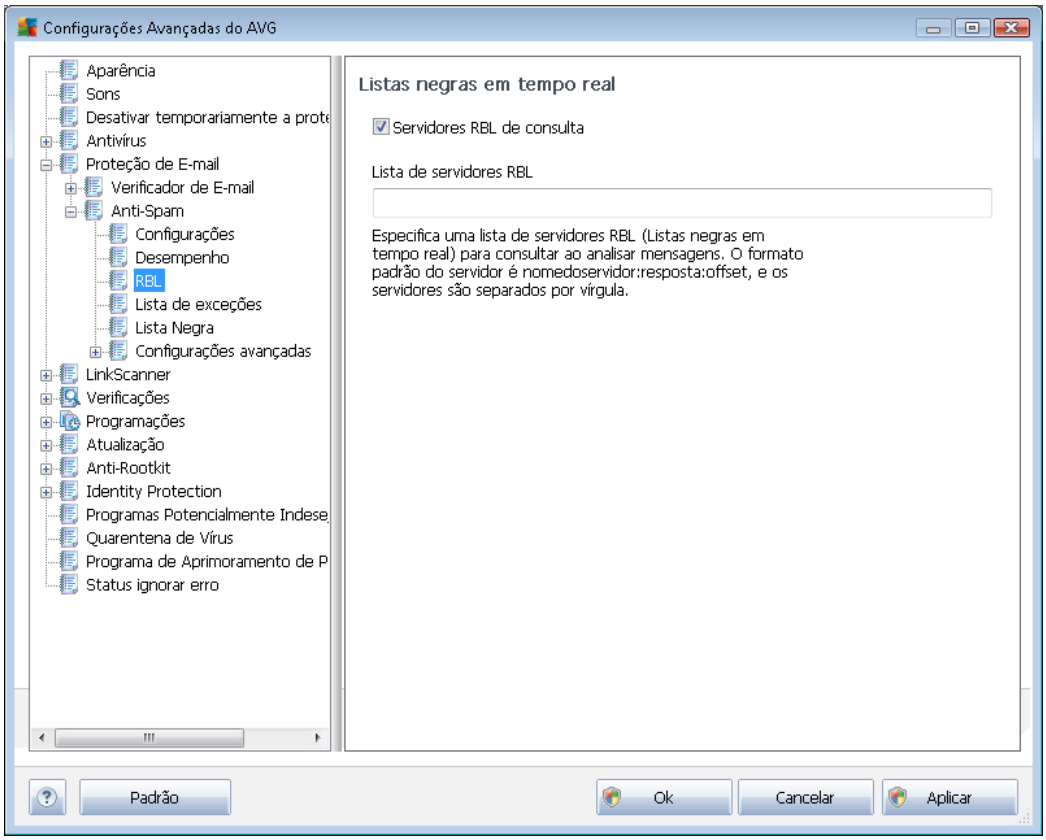
- ***Pouca memória*** - durante o processo de verificação para identificar spam, nenhuma regra será usada. Apenas os dados de treinamento serão usados para identificação. Esse modo não é recomendado para uso comum, a menos que o hardware do computador seja realmente fraco.

- ***Alto desempenho*** - este modo consumirá muita memória. Durante o processo de verificação para identificar um spam, os seguintes recursos serão usados: cache do banco de dados de regras e spam, regras básicas e avançadas, endereços IP de spam e bancos de dados de spam.

O item ***Habilitar verificação online*** fica ativado por padrão. Ele resulta em uma detecção de spam mais precisa por meio da comunicação com os servidores Mailshell, ou seja, os dados verificados serão comparados com o banco de dados Mailshell on-line.

Geralmente é recomendável manter as configurações padrão e alterá-las somente se houver um motivo para isso. Alterações na configuração devem ser feitas somente por usuários experientes!

O item ***RBL*** abre uma caixa de diálogo de edição chamada ***Listas negras em tempo real***, onde você pode ativar/desativar a função***Servidores RBL de consulta***:

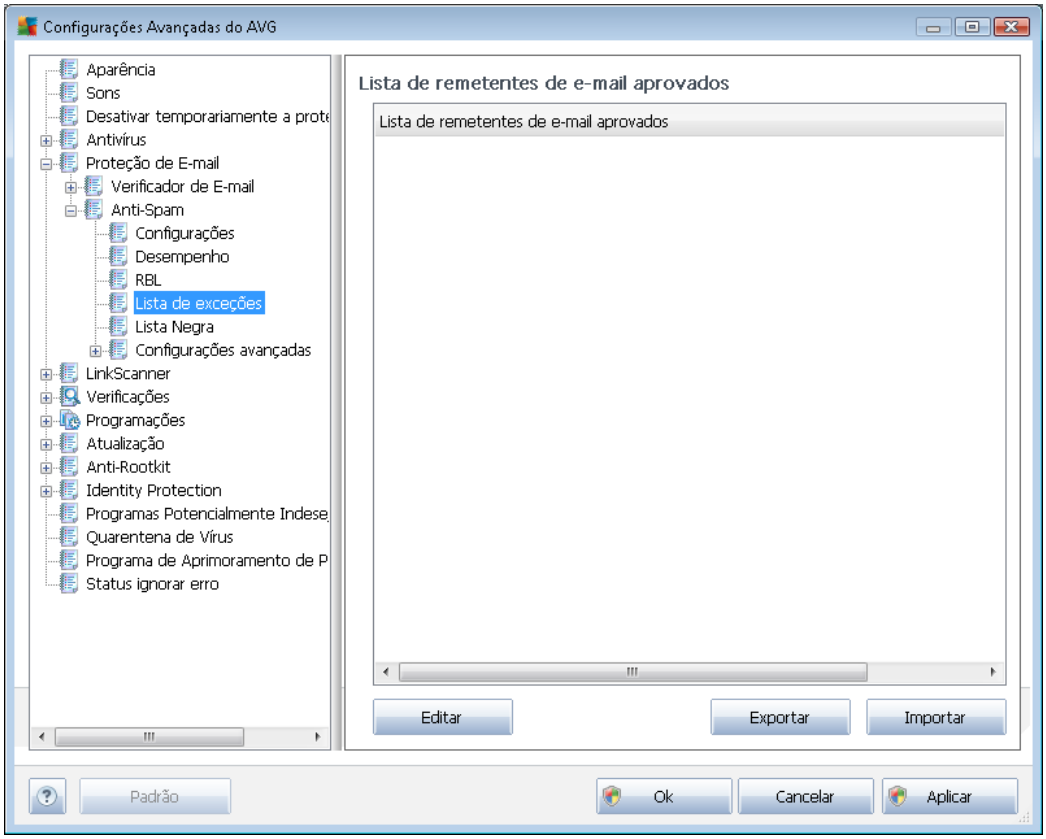


O servidor RBL (*Realtime Blackhole Lists*) é um servidor DNS com um amplo banco de dados de remetentes de spam. Quando esse recurso estiver ativado, todas as mensagens de e-mail serão verificadas no banco de dados do servidor RBL e marcadas como spam, se forem idênticas a qualquer uma das entradas do banco de dados. Os bancos de dados dos servidores RBL contêm as impressões de spam atualizadas por minuto, mais recentes, para fornecer a melhor e mais precisa detecção de spam. Esse recurso é especialmente útil para usuários que recebem grandes quantidades de spam que não estão sendo detectados normalmente pelo mecanismo Anti-Spam.

A ***Lista de servidores RBL***permite que você defina locais específicos do servidor RBL (*a ativação desse recurso pode tornar lento o processo de recebimento de e-mails em alguns sistemas e configurações, já que todas as mensagens devem ser verificadas pelo banco de dados do servidor RBL).*

Nenhum dado pessoal é enviado ao servidor!

O item ***Lista de exceções*** abre uma caixa de diálogo denominada ***Lista de remetentes de e-mail aprovados***, com uma lista global de endereços de e-mail e nomes de domínio de remetentes aprovados cujas mensagens nunca serão marcadas como spam.



Na interface de edição, você pode compilar uma lista dos remetentes sobre os quais tem certeza de que não enviarão mensagens indesejáveis (spam). Você pode também compilar uma lista de nomes de domínio completos (*como avg.com*) que você sabe que não gera mensagens de spam. Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los digitando diretamente cada endereço de e-mail ou importando toda a lista de endereços de uma vez.

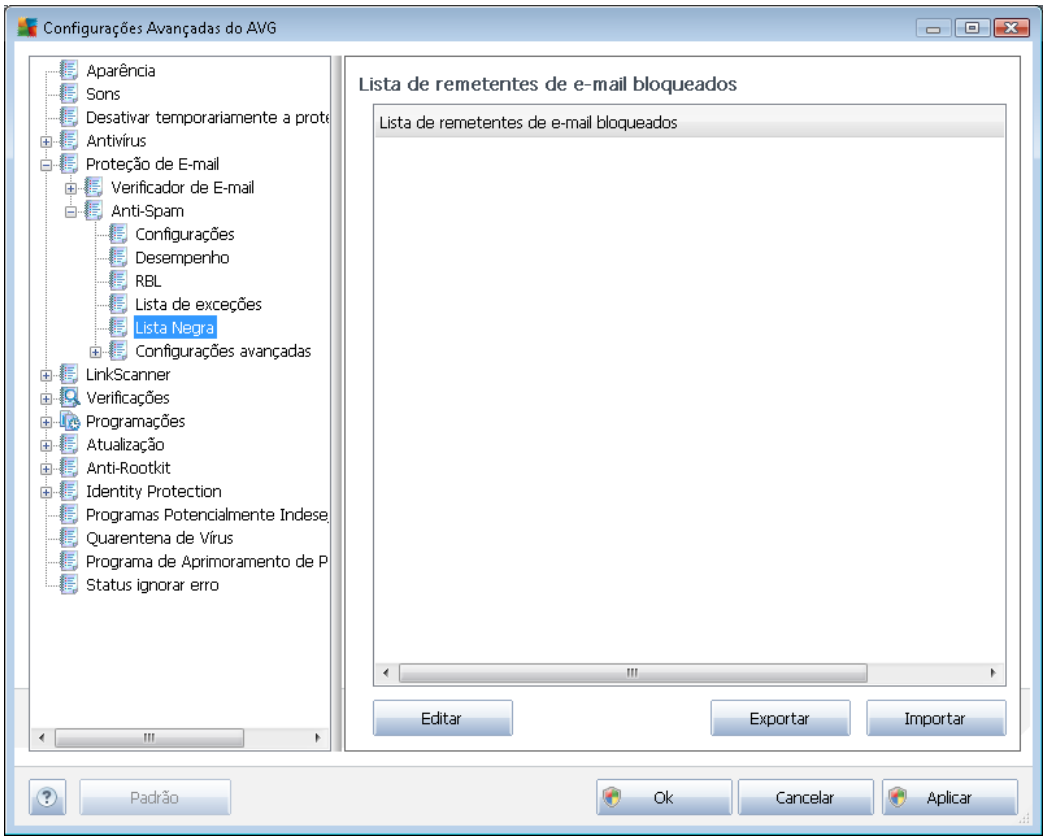
Botões de controle

Os seguintes botões estão disponíveis:

- ***Editar*** - pressione esse botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (*você também pode usar o método copiar/colar*). Insira um item (*remetente, nome do domínio*) por linha.
- ***Exportar*** - se, por algum motivo, você decidir exportar os registros, será possível fazê-lo pressionando esse botão. Todos os registros serão salvos em um arquivo de texto simples.
- ***Importar*** - se você já tiver um arquivo de texto com nomes de domínio/endereços de e-mail

preparado, poderá simplesmente importá-lo selecionando este botão. O conteúdo do arquivo deve conter somente um item (*endereço, nome de domínio*) por linha.

O item ***Lista negra*** abre uma caixa de diálogo com uma lista global de endereços de e-mail e nomes de domínio de remetentes bloqueados cujas mensagens sempre serão marcadas como spam.



Na interface de edição, você pode compilar uma lista dos remetentes que você espera que enviem mensagens indesejáveis *(spam)*. Você também pode compilar uma lista de nomes de domínio completos (*como empresaqueenviaspam.com*), dos quais espera receber mensagens de spam. Todos os endereços de e-mail/domínios listados serão identificados como spam. Depois de preparar essa lista de remetentes e/ou nomes de domínio, você poderá inseri-los digitando diretamente cada endereço de e-mail ou importando toda a lista de endereços de uma vez.

Botões de controle

Os seguintes botões estão disponíveis:

- ***Editar*** - pressione esse botão para abrir uma caixa de diálogo na qual é possível inserir manualmente uma lista de endereços (*você também pode usar o método copiar/colar*). Insira um item (*remetente, nome do domínio*) por linha.

- ***Exportar*** - se, por algum motivo, você decidir exportar os registros, será possível fazê-lo pressionando esse botão. Todos os registros serão salvos em um arquivo de texto simples.

- ***Importar*** - se você já tiver um arquivo de texto com nomes de domínio/endereços de e-mail preparado, poderá simplesmente importá-lo selecionando este botão.

A seção Configurações avançadas contém várias opções de configuração para o componente Anti-Spam. Essas configurações se destinam exclusivamente a usuários experientes, principalmente administradores de rede, que precisam configurar a proteção antispam em detalhes para melhor proteger os servidores de e-mail. Por essa razão, não há ajuda adicional disponível para as caixas de diálogo individuais; entretanto, existe uma breve descrição de cada opção respectiva diretamente na interface do usuário.

É altamente recomendável não alterar as configurações, a menos que você esteja bastante familiarizado com as configurações avançadas do Spamcatcher (MailShell Inc.). Qualquer alteração inapropriada poderá resultar em mau desempenho ou no funcionamento incorreto do componente.

Se você ainda acredita que precisa alterar as configurações Anti-Spam no nível muito avançado, siga as instruções fornecidas diretamente na interface do usuário. Geralmente, em cada caixa de diálogo você encontrará um único recurso específico e poderá editá-lo. Sua descrição é sempre incluída na caixa.

- ***Cache*** - impressão digital, reputação do domínio, LegitRepute

- ***Treinamento*** - máximo de entradas de palavras, limite de treinamento automático, peso

- ***Filtragem*** - lista de idiomas, lista de países, IPs aprovados, IPs bloqueados, países bloqueados, conjunto de caracteres bloqueados, remetentes falsificados

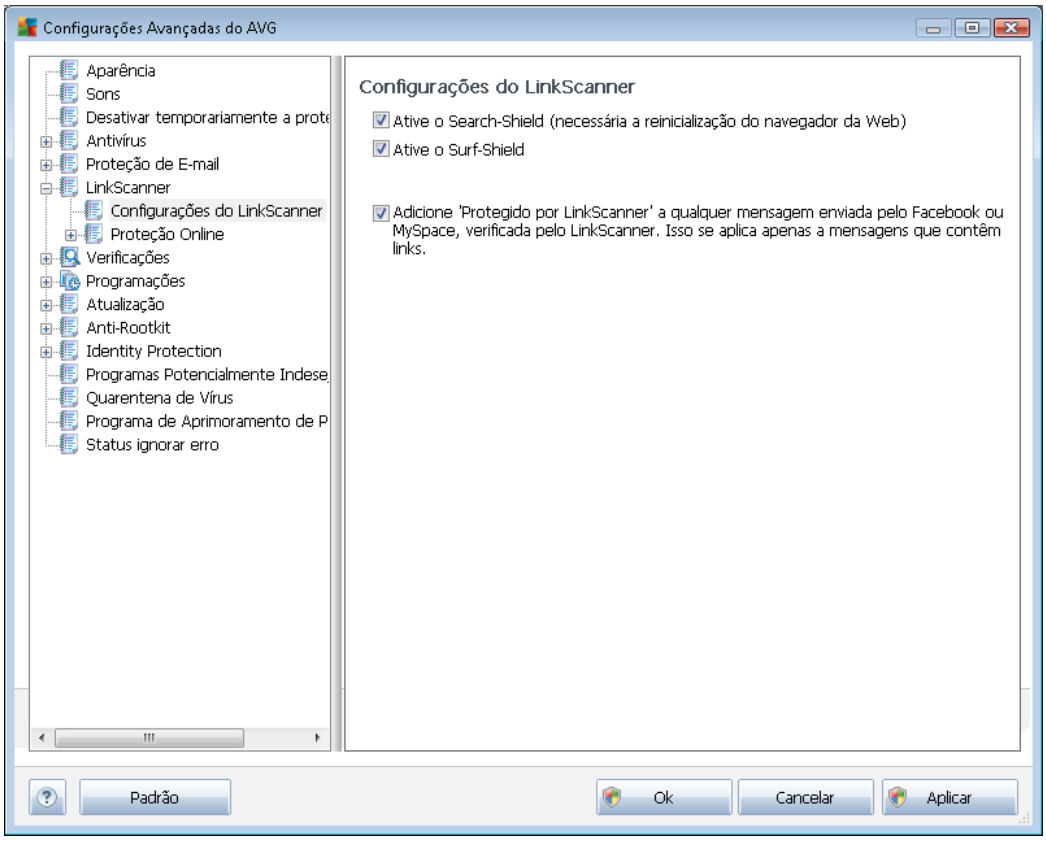
- ***RBL*** - servidores RBL, vários acertos, limite, tempo limite, máximo de IPs

- ***Conexão com a Internet*** - tempo limite, servidor proxy, autenticação proxy

9.6. Link Scanner

9.6.1. Configurações do Verificador de link

A caixa de diálogo ***Configurações do LinkScanner*** permite ativar ou desativar os recursos básicos do LinkScanner:

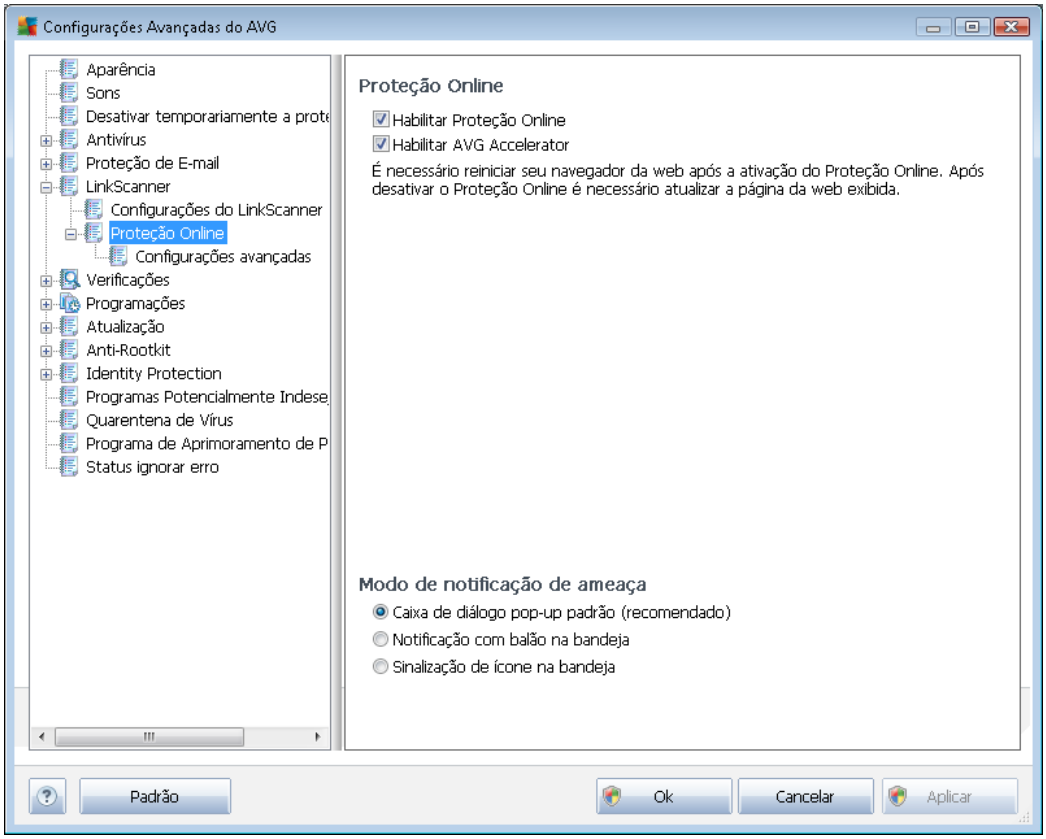


- ***Habilitar o Search-Shield*** - (*por padrão*): ícones de notificação consultiva em buscas realizadas com o Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ou SlashDot: verificarão adiante o conteúdo dos sites retornados pelo mecanismo de busca.

- ***Ativar Surf-Shield*** - (*ativo por padrão*): proteção ativa (*em tempo real*) contra sites exploradores à medida que são acessados. As conexões conhecidas com sites maliciosos e seu conteúdo exploratório são bloqueadas à medida que são acessados por meio de um navegador da Web *ou outro aplicativo que utilize HTTP*).

- ***Adicionar "Protegido pelo LinkScanner"...*** - (*ativado por padrão*): marque este item para confirmar que deseja inserir o aviso de certificação na verificação de todas as mensagens do Link Scanner que contêm hiperlinks ativos enviados a partir das redes sociais Facebook e MySpace.

9.6.2. Proteção On-line



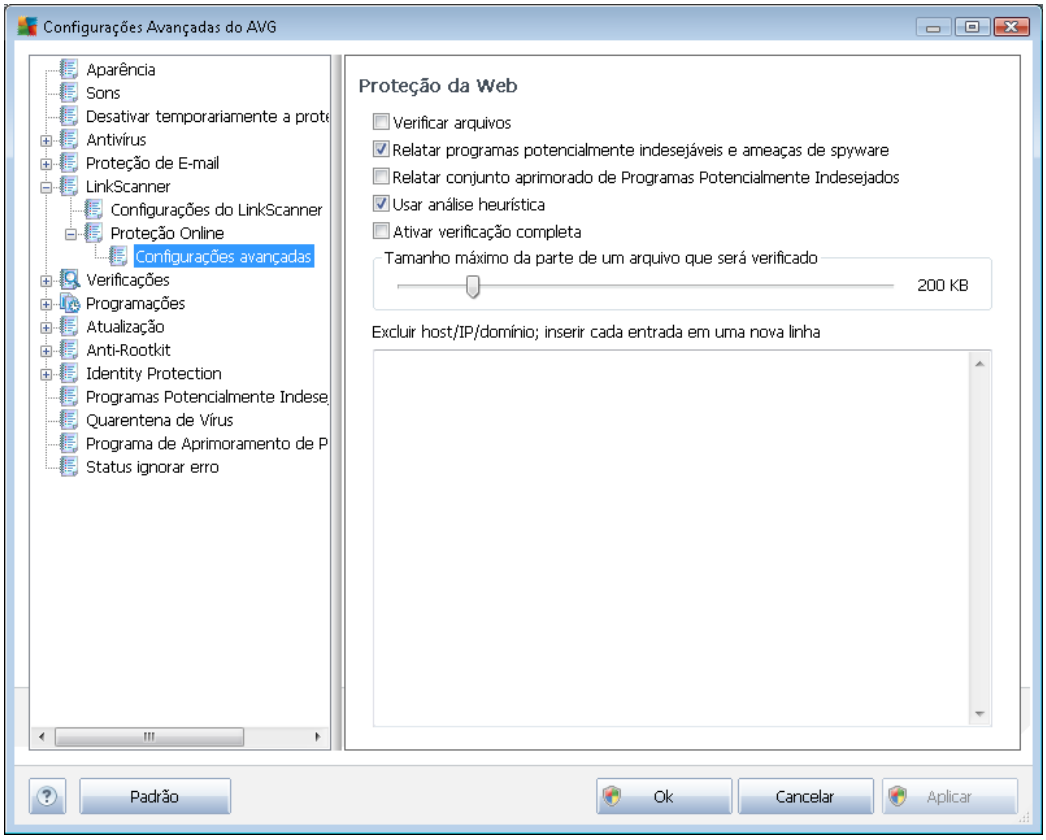
A caixa de diálogo ***Proteção Online*** oferece as seguintes opções:

- ***Habilitar Proteção Online****(ativado por padrão)* - ativa/desativa todo o serviço da ***Proteção Online***. Para obter mais configurações avançadas da ***Proteção Online***, siga para a caixa de diálogo seguinte: Proteção da Web.

- ***Habilitar o AVG Accelerator*** *(ativado por padrão)* - ativa/desativa o serviço ***AVG Accelerator***, que melhora a reprodução de vídeos online e facilita a execução de downloads adicionais.

Modo de notificação de ameaça

Na parte inferior da caixa de diálogo, selecione de que maneira você gostaria de ser informado sobre possíveis ameaças detectadas: por meio de uma caixa de diálogo pop-up, notificação de balão na bandeja ou nas informações de ícone na bandeja.



Na caixa de diálogo ***Proteção da Web***, você pode editar a configuração do componente com relação à verificação do conteúdo do site da Web. A interface de edição permite configurar as seguintes opções elementares:

- ***Ativar Proteção da Web*** - essa opção confirma que o ***Proteção Online*** deve realizar a verificação do conteúdo das páginas www. Desde que essa opção esteja ativada (*por padrão*), você pode ativar/desativar estes itens:
    - ***Verificar arquivos*** - (*desativada por padrão*): verifique o conteúdo dos arquivos possivelmente incluídos na página www a ser exibida.
    - ***Informar programas potencialmente indesejáveis e ameaças de spyware*** - (*ativado por padrão*) marque para ativar o mecanismo Anti-Spyware e verificar se há vírus e spyware. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.
    - ***Informar conjunto avançado de programas potencialmente indesejáveis*** - (*desativada por padrão*): marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda

mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Usar análise heurística*** - (*ativada por padrão*): verifique o conteúdo da página a ser exibida usando o método de análise heurística (*emulação dinâmica das instruções do objeto verificado em um ambiente de computador virtual*).

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- ***Tamanho máximo de um arquivo a ser verificado*** - se os arquivos incluídos estiverem presentes na página exibida, você também poderá verificar o conteúdo deles, mesmo antes que serem baixados para seu computador. Entretanto, a verificação de arquivos grandes pode levar tempo e o download da página da Web pode ficar significativamente mais lento. Use a barra deslizante para especificar o tamanho máximo de um arquivo que ainda será verificado pela ***Proteção Online***. Mesmo se o arquivo baixado for maior que o especificado, deixando de ser verificado pela Proteção Online, você ainda estará protegido. Se o arquivo estiver infectado, a ***Proteção Residente*** o detectará imediatamente.

- ***Excluir host/IP/domínio*** - no campo de texto você pode digitar o nome exato de um servidor (*host, endereço IP, endereço IP com máscara ou URL*) ou um domínio que não deve ser verificado pela ***Proteção Online***. Portanto, exclua apenas o host que você tenha certeza de que nunca permitirá conteúdo web perigoso.

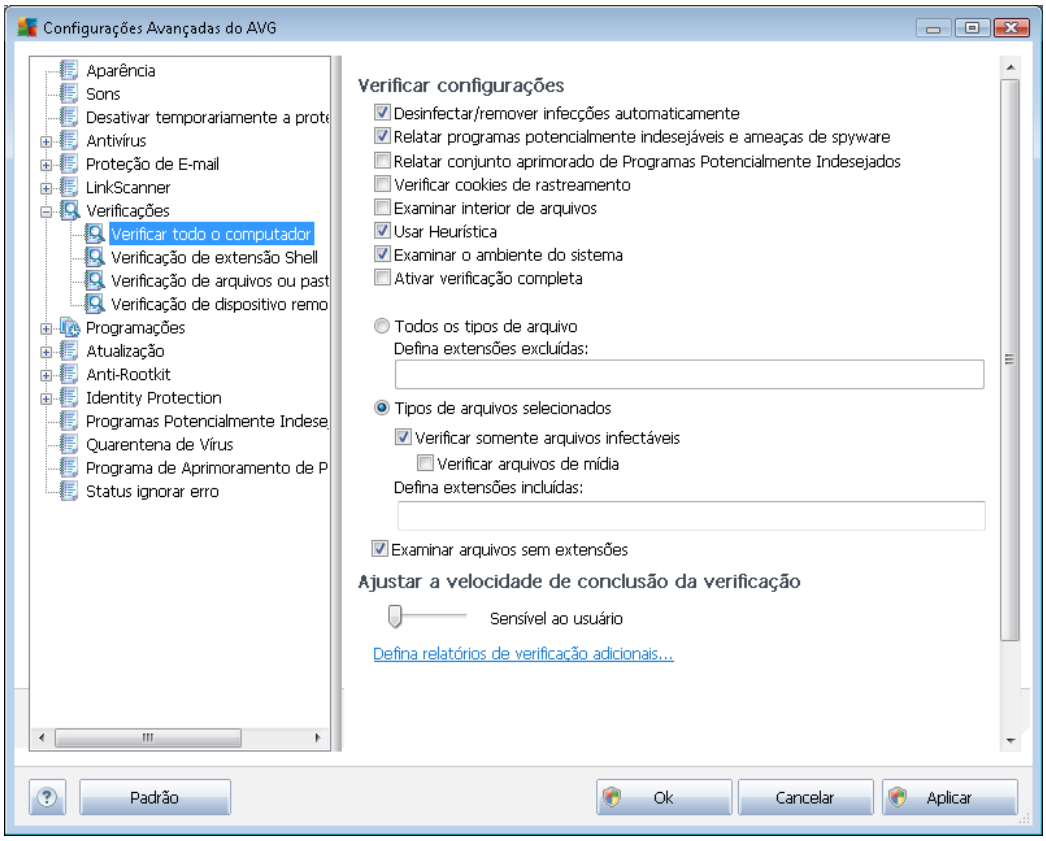
9.7. Verificações

As configurações de verificação avançadas estão divididas em três categorias referentes a tipos específicos de verificação, conforme definido pelo fornecedor do software:

- ***Verificar todo o computador*** - verificação padrão predefinida de todo o computador
- ***Verificação de extensão Shell*** - verificação específica de um objeto selecionado diretamente do ambiente do Windows Explorer
- ***Verificação de arquivos ou pastas específicas*** - verificação padrão predefinida de áreas selecionadas do computador
- ***Verificação de dispositivos removíveis*** - verificação específica de dispositivos removíveis conectados ao computador

9.7.1. Verificação de todo o computador

A opção ***Verificar todo o computador*** permite a edição de parâmetros de uma das verificações predefinidas pelo fornecedor do software, Verificar todo o computador:



Configurações da verificação

Na guia ***Configurações da verificação*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados.

- ***Reparar ou remover infecção automaticamente*** (*ativada por padrão*) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo Anti-Spyware e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada*

por padrão) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*) - este parâmetro do componente Anti-Spyware define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*)

- ***Verificar dentro dos arquivos*** (*desativada por padrão*) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

- ***Usar Heurística*** (*ativada por padrão*) - a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***Verificar ambiente do sistema*** (*ativada por padrão*) - a verificação também atuará nas áreas do sistema do seu computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

Além disso, você deve decidir se deseja verificar

- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas) que não devem ser verificadas;

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

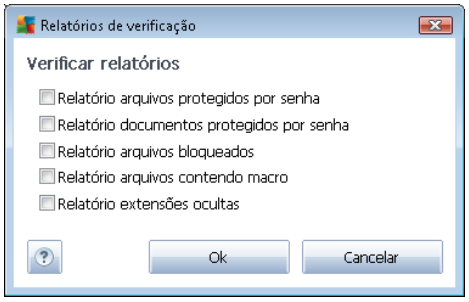
- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

Ajustar a velocidade de conclusão da verificação

Na seção ***Ajustar a velocidade de conclusão da verificação***, você poderá especificar a velocidade de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos do sistema será bem maior durante sua execução e as outras atividades do PC terão o desempenho reduzido (*essa opção pode ser usada quando o computador está ligado, mas ninguém está trabalhando nele*). Por outro lado, você pode diminuir a utilização dos recursos do sistema ampliando a duração da verificação.

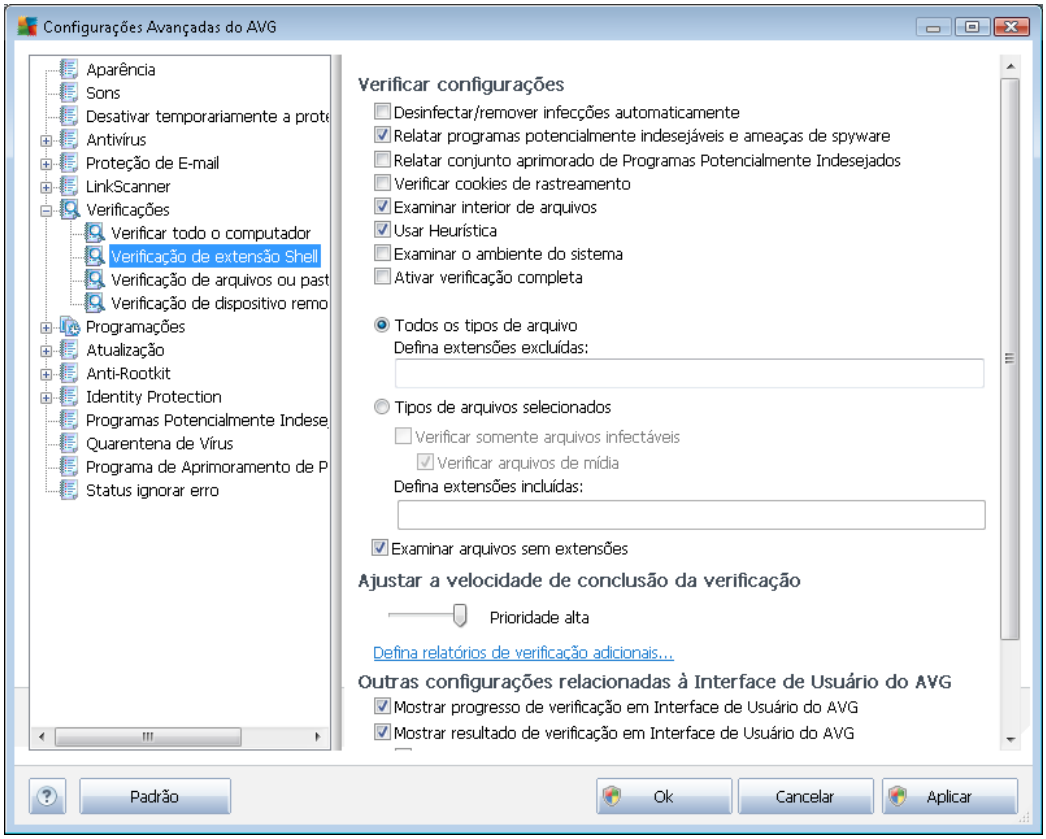
Defina relatórios de verificação adicionais...

Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



9.7.2. Verificação da extensão Shell

Da mesma forma que o item anterior, Verificar todo o computador , este item, denominado ***Verificação da extensão shell*** também oferece várias opções para editar a verificação predefinida pelo fornecedor do software. Dessa vez a configuração é relacionada à verificação de objetos específicos inicializados diretamente no ambiente do Windows Explorer (*extensão shell*). Consulte o capítulo Verificação do Windows Explorer:



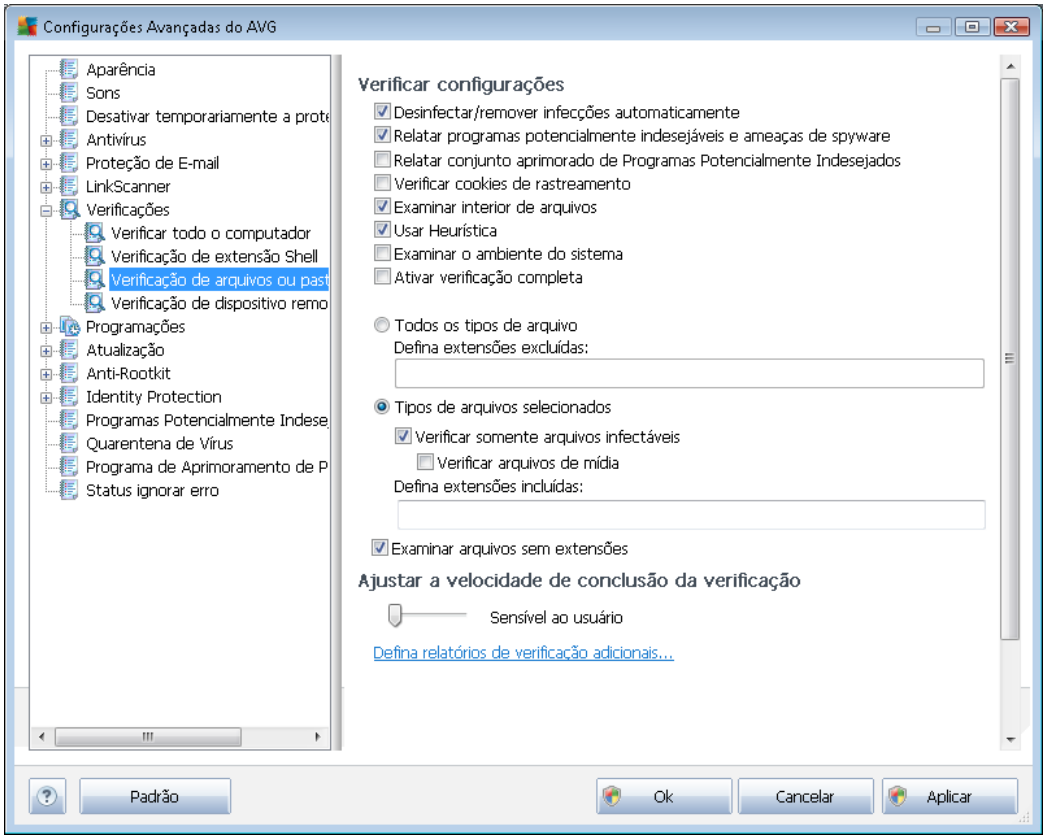
A lista de parâmetros é idêntica à disponível para Verificar todo o computador. Entretanto, as configurações padrão são diferentes (*por exemplo, Verificar todo o computador, por padrão, não verifica os arquivos, mas verifica o ambiente de sistema, ao passo que com a Verificação da Extensão Shell, é ao contrário*).

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo Configurações avançadas do AVG/Verificações/Verificar todo o computador.*

Em comparação com a caixa de diálogo Verificar todo o computador, a caixa de diálogo ***Verificação da extensão Shell*** também tem uma seção denominada ***Outras configurações relacionadas à interface do usuário do AVG***, onde você pode especificar se deseja que o progresso da verificação e os resultados da verificação estejam acessíveis na interface do usuário do AVG. Além disso, você pode definir que o resultado da verificação seja exibido apenas se uma infecção for detectada durante a verificação.

9.7.3. Verificação de arquivos ou pastas específicas

A interface de edição de ***Verificar arquivos ou pastas específicos*** é idêntica à caixa de diálogo de edição Verificar todo o computador. Todas as opções de configuração são as mesmas, porém as configurações padrão são mais rigorosas em Verificar todo o computador.

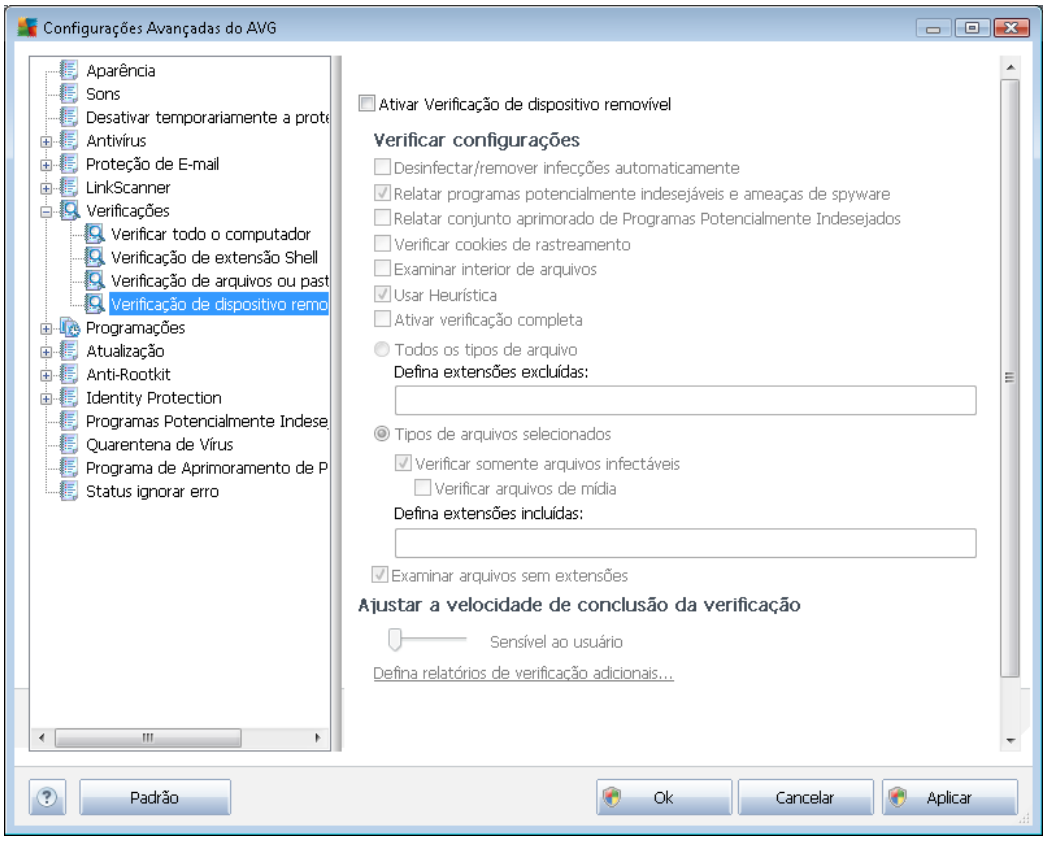


Todo os parâmetros definidos nesta caixa de diálogo de configuração são válidos somente para as áreas selecionadas para verificação com a Verificação de arquivos ou pastas específicos!

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo Configurações avançadas do AVG/Verificações/Verificar todo o computador.*

9.7.4. Verificação de dispositivo removível

A interface de edição de ***Verificação de dispositivo removível*** também é muito semelhante à caixa de diálogo de edição Verificar todo o computador:



A ***Verificação de dispositivo removível*** é ativada automaticamente quando você conecta um dispositivo removível ao computador. Por padrão, essa verificação está desativada. No entanto, é essencial verificar dispositivos removíveis em busca de ameaças potenciais, pois são uma das fontes principais de infecção. Para que a verificação esteja pronta e seja iniciada quando necessário, marque a opção ***Ativar verificação de dispositivo removível*** .

Observação:*para obter uma descrição dos parâmetros específicos, consulte o capítulo Configurações avançadas do AVG/Verificações/Verificar todo o computador.*

9.8. Programações

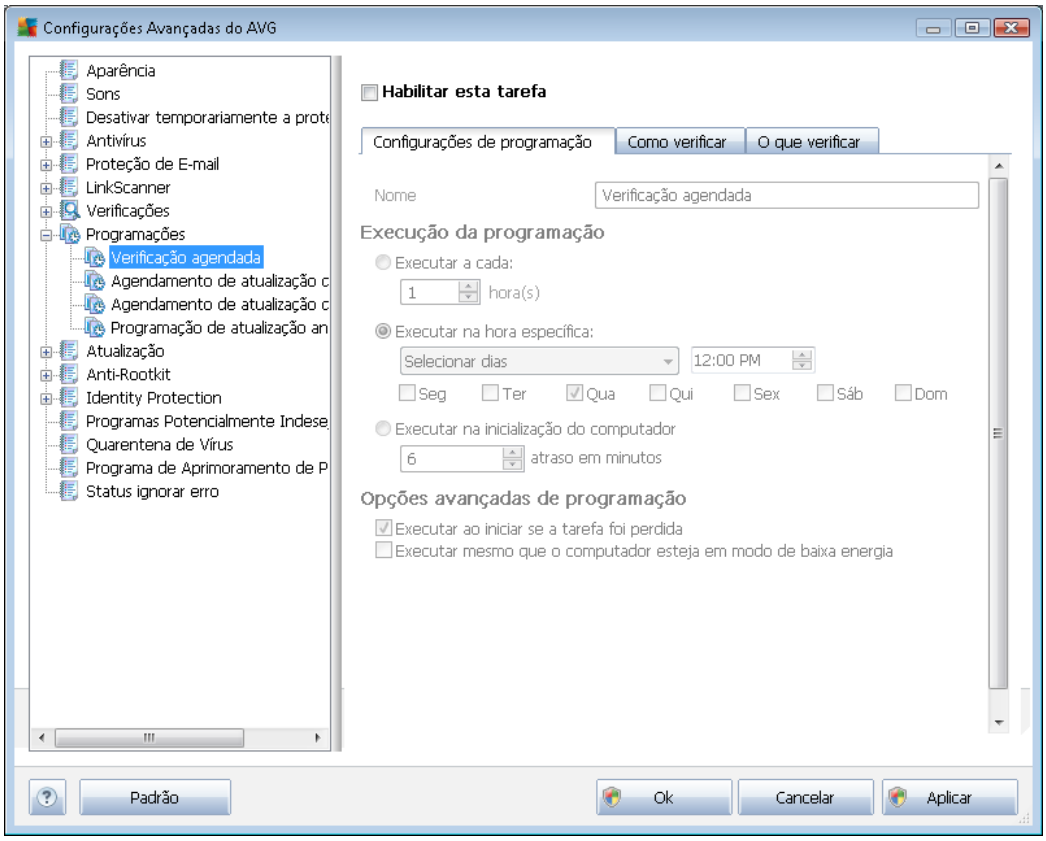
Na seção ***Agendamentos***, é possível editar as configurações padrão de:

- Verificação agendada
- Agendamento de atualização de definições
- Agendamento de atualização de programa

- Agendamento de atualização do Anti-Spam

9.8.1. Verificação programada

Os parâmetros da verificação agendada podem ser editados(*ou uma nova configuração de agenda*) em três guias. Em cada guia, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente o teste agendado e ativá-lo novamente quando necessário:



Em seguida, no campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa. Para programações recém-adicionadas (*é possível adicionar uma nova programação clicando com o botão direito no item* ***Verificação programada*** *na área de navegação esquerda*), você pode especificar o seu próprio nome e, nesse caso, o campo de texto ficará aberto para edição. Tente sempre usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

Exemplo: *não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc. Além disso, não é necessário especificar no nome da verificação se ela é uma verificação de todo o computador ou somente uma verificação de pastas ou arquivos selecionados. Suas verificações serão sempre uma versão específica da verificação de arquivos ou pastas selecionados.*

Nessa caixa de diálogo você ainda poderá definir os seguintes parâmetros de verificação:

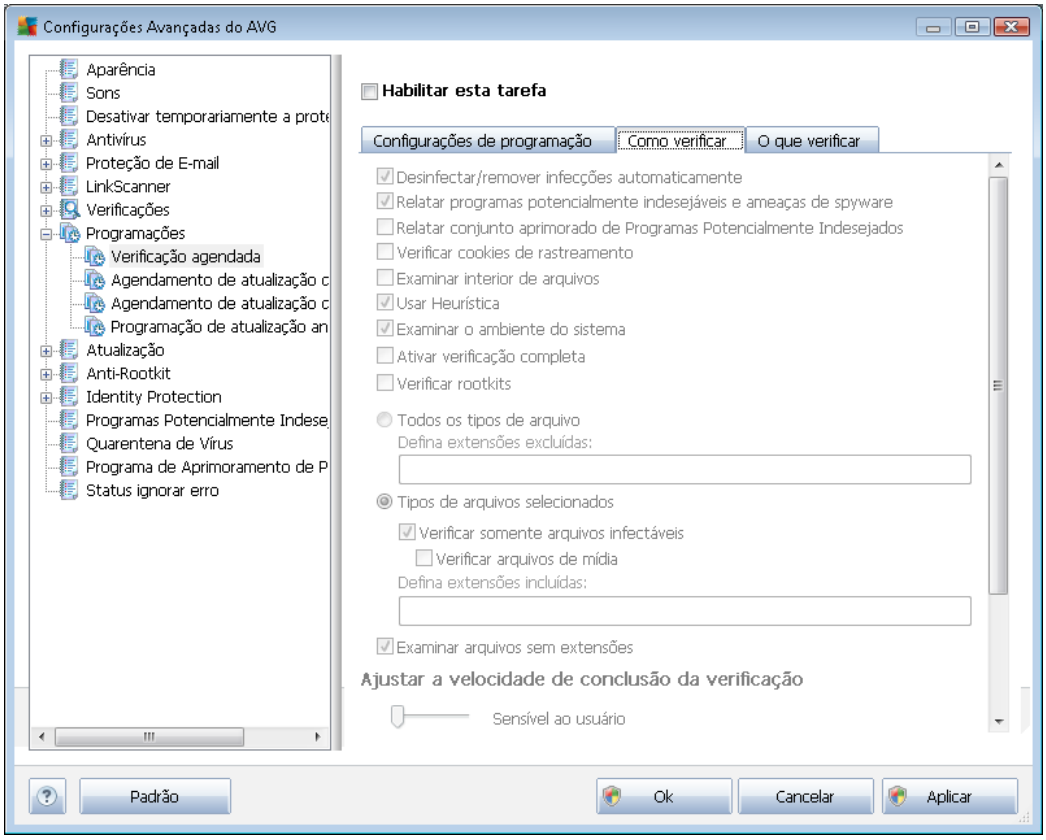
Execução da programação

Aqui, você pode especificar intervalos de tempo para a ativação da verificação recém-programada. O tempo pode ser definido pela repetição da execução da verificação depois de um determinado período (***Executar a cada ...***), pela definição de uma data e hora exatas (***Executar em uma hora específica...***) ou talvez pela definição de um evento ao qual a ativação da verificação deve ser associada (***Executar na inicialização do computador***).

Opções avançadas de programação

Essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado. Uma vez que a verificação agendada é iniciada no horário que você especificou, você será informado deste fato por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema:

Um novo ícone AVG na bandeja do sistema aparece (*em cores e com um holofote*) informando que uma verificação agendada está em execução. Clique com o botão direito do mouse no ícone AVG da verificação em execução para abrir um menu de contexto, onde você pode escolher pausar ou até interromper a verificação e também alterar a prioridade da verificação em execução:



Na guia ***Como verificar*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros é ativada e a funcionalidade será aplicada durante a verificação. ***A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida***:

- ***Reparar ou remover vírus automaticamente*** *(ativado por padrão):* se um vírus for identificado durante a verificação, ele poderá ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware*** *(ativada por padrão):* marque para ativar o mecanismo Anti-Spyware e verificar se há spyware, bem como vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*): marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*): este parâmetro do componente Anti-Spyware define que os cookies devem ser detectados durante a verificação; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*)

- ***Verificar interior dos arquivos*** (*desativada por padrão*): este parâmetro define que a verificação deve atuar em todos os arquivos, mesmo que eles estejam compactados em algum tipo de arquivo, como ZIP, RAR etc.

- ***Usar Heurística*** (*ativada por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação;

- ***Verificar ambiente do sistema*** (*ativada por padrão*): a verificação também atuará nas áreas do sistema do seu computador;

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- ***Verificar rootkits*** (*desativada por padrão*): marque este item se desejar incluir a detecção de rootkit na verificação de todo o computador. A detecção de rootkit também está disponível por meio do componente Anti-Rootkit;

Além disso, você deve decidir se deseja verificar

- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula (sendo salvas, as vírgulas mudam para ponto-e-vírgulas)

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

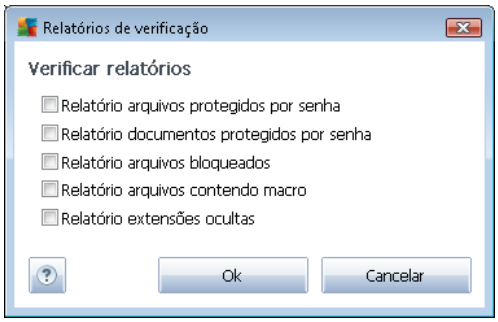
Ajustar a velocidade de conclusão da verificação

Na seção ***Ajustar a velocidade de conclusão da verificação***, você poderá especificar a velocidade

de verificação desejada, dependendo do uso do recurso do sistema. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. A verificação poderá ser acelerada, mas a utilização de recursos do sistema será bem maior durante sua execução e as outras atividades do PC terão o desempenho reduzido (*essa opção pode ser usada quando o computador está ligado, mas ninguém está trabalhando nele*). Por outro lado, você pode diminuir a utilização dos recursos do sistema ampliando a duração da verificação.

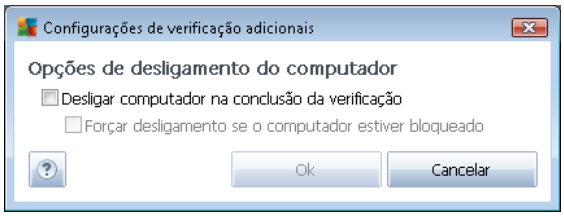
Defina relatórios de verificação adicionais

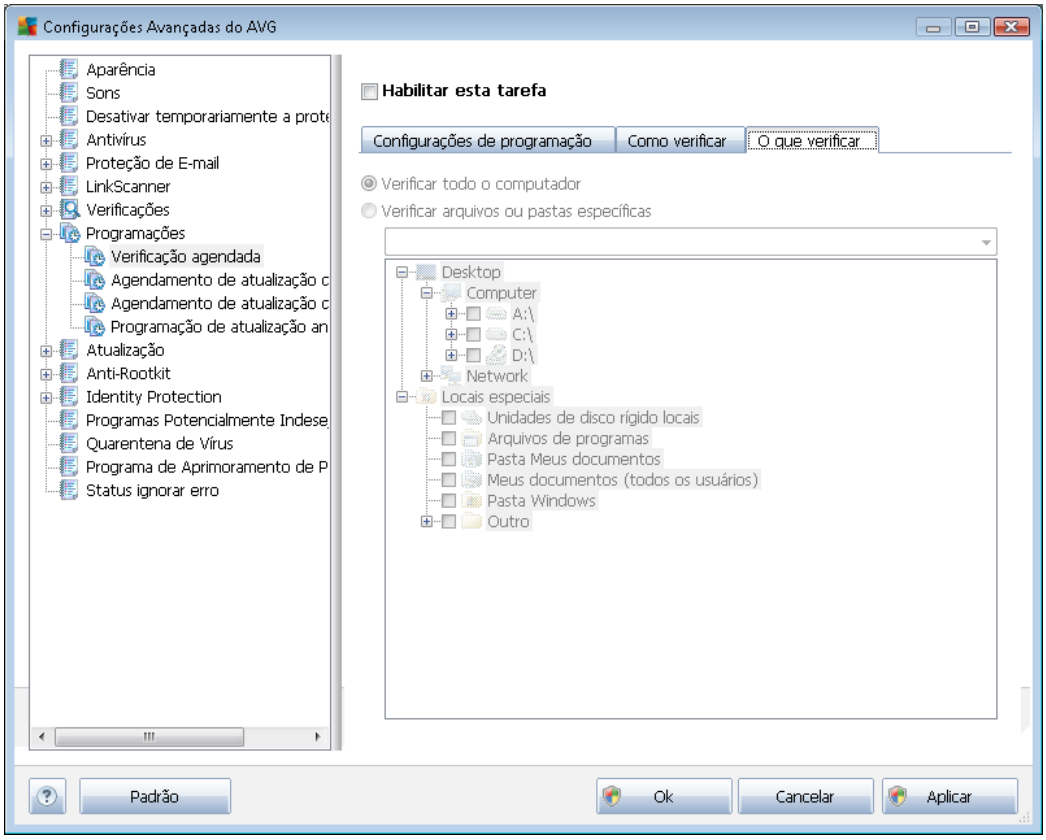
Clique no link ***Definir relatórios de verificação adicionais...*** para abrir uma janela independente da caixa de diálogo chamada ***Verificar relatórios*** na qual você pode marcar vários itens para definir quais localizações da verificação devem ser relatadas:



Configurações de verificação adicionais

Clique em ***Configurações de verificação adicionais ...*** para abrir uma nova caixa de diálogo ***Opções de desligamento do computador*** que permite decidir se o computador deve ser desligado automaticamente assim que o processo de verificação estiver terminado. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo se ele estiver bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

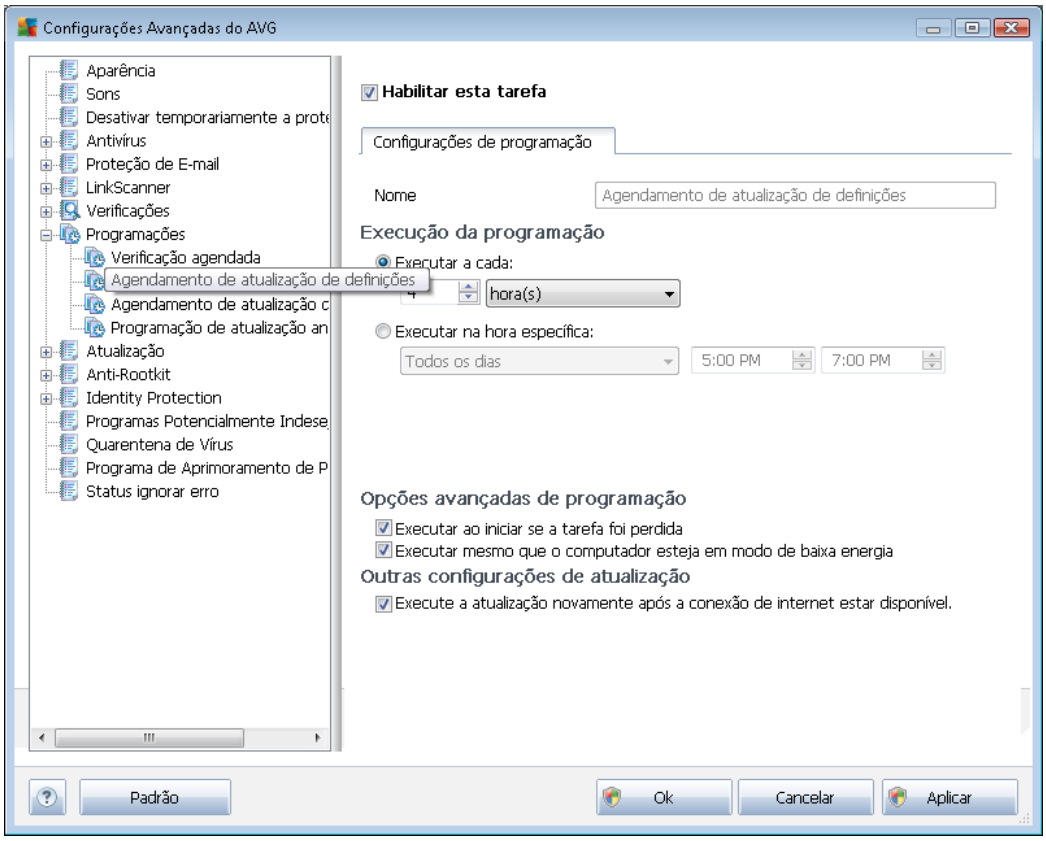




Na guia ***O que verificar***, você pode definir se deseja programar a verificação de todo o computador ou a verificação de arquivos ou pastas específicas. Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação.

9.8.2. Agendamento de atualização de definições

Se for ***realmente necessário***, você pode desmarcar o item ***Ativar esta tarefa*** para desativar temporariamente a atualização de definições programada e ativá-la novamente mais tarde:



Nesta caixa de diálogo, você pode configurar alguns parâmetros detalhados do agendamento de atualização de definições. No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Nesta seção, especifique os intervalos de tempo para a execução da atualização de definições recém-agendada. O prazo pode ser definido pelo início repetido de atualização após certo período de tempo (***Executar a cada...***) ou definindo um data e hora exatos (***Executar na hora específica...***).

Opções avançadas de programação

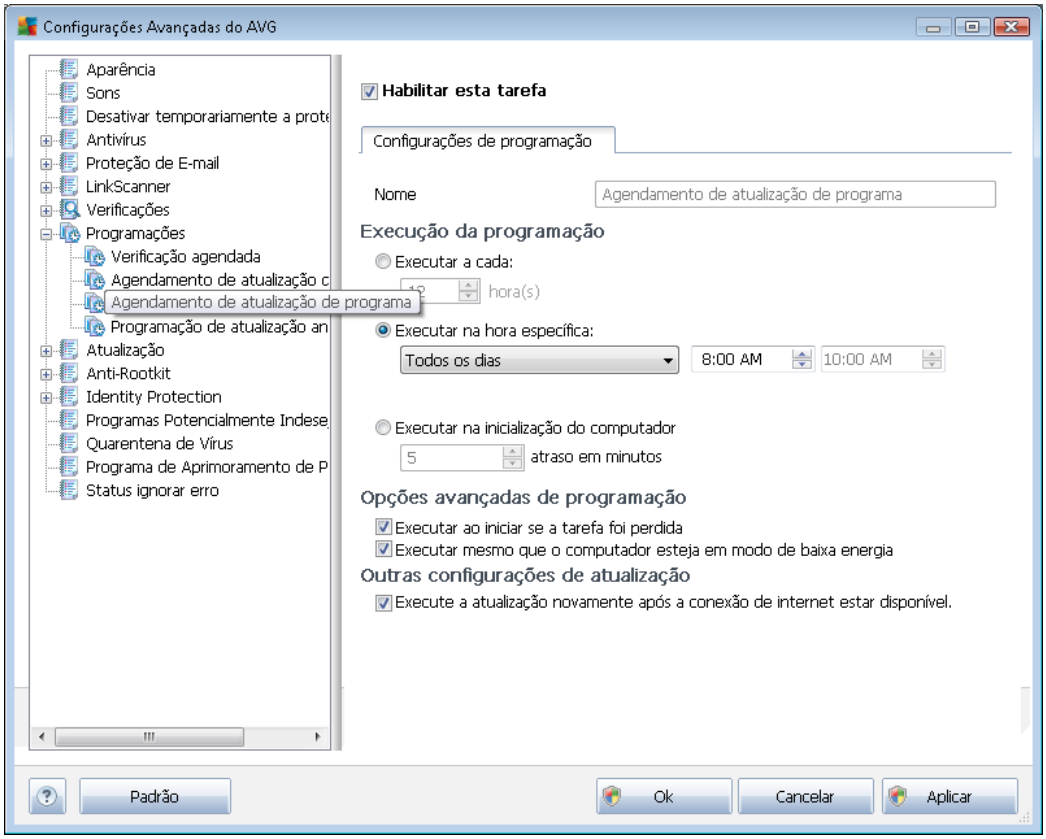
Esta seção permite definir sob quais condições a atualização de definições deverá ou não ser executada se o computador estiver no modo de pouca energia ou completamente desligado.

Outras configurações de atualização

Por fim, marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada. Assim que a atualização programada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo Configurações avançadas/Aparência*).

9.8.3. Agendamento de atualização de programa

Se for ***realmente necessário***, você pode desmarcar o item ***Ativar essa tarefa*** para simplesmente desativar temporariamente o programa de atualização agendado, ativando-o mais tarde novamente:



No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Aqui, especifique os intervalos de tempo para iniciar a atualização do programa recém-programada. O tempo pode ser definido pela repetição da inicialização da atualização depois de um determinado período (***Executar a cada...***), pela definição de uma data e hora exatas (***Executar em uma hora***

específica...) ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (***Ação baseada na inicialização do computador***).

Opções avançadas de programação

Essa seção permite definir sob quais condições a atualização do programa deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

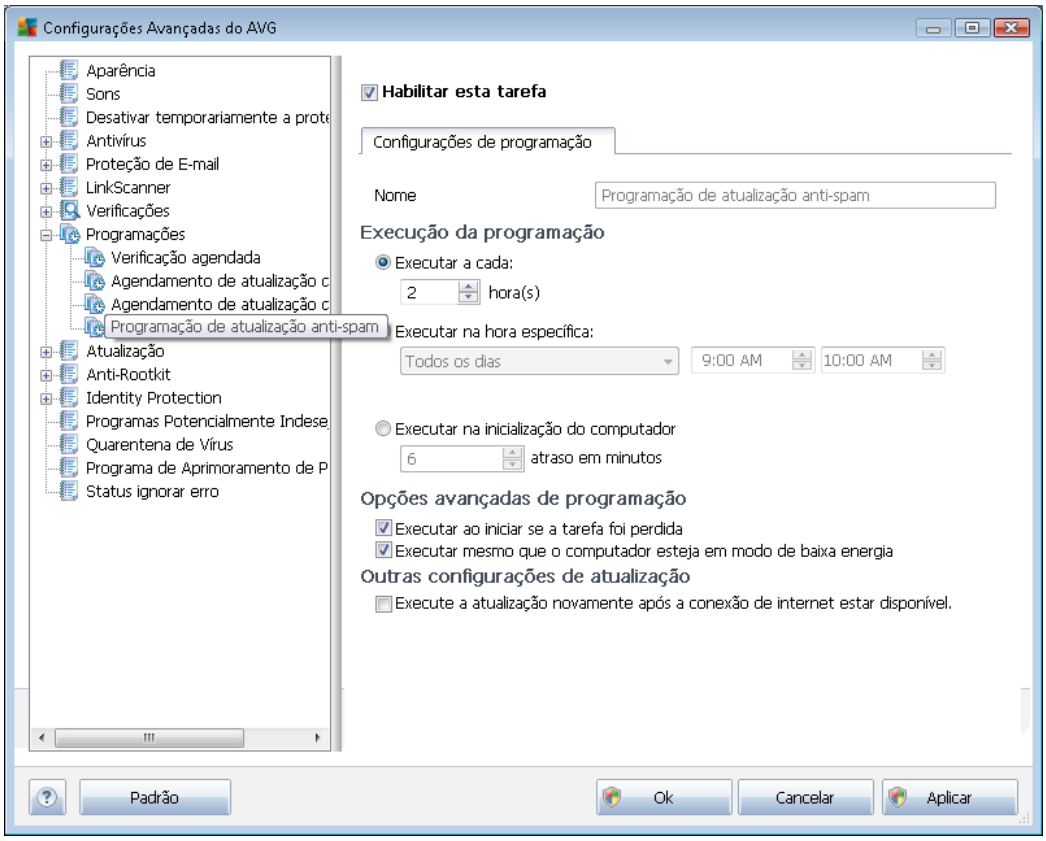
Outras configurações de atualização

Marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível***, para ter certeza de que, se a conexão com a Internet ficar corrompida e o processo de atualização falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada. Assim que a atualização programada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone do AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo Configurações avançadas/Aparência*).

Observação: *se ocorrer uma coincidência de tempo de uma atualização de programa agendada e uma verificação agendada, o processo de atualização terá maior prioridade, e a verificação será interrompida.*

9.8.4. Agendamento de atualização do anti-spam

Se for realmente necessário, você poderá desmarcar o item ***Ativar esta tarefa*** para simplesmente desativar a atualização programada do Anti-Spam temporariamente e reativá-lo mais tarde:



Nessa caixa de diálogo, você pode configurar parâmetros detalhados do programa de atualização. No campo de texto denominado ***Nome*** (*desativado para todas as programações padrão*), existe o nome atribuído a essa programação pelo fornecedor do programa.

Execução da programação

Aqui, especifique os intervalos de tempo para a inicialização da atualização do Anti-Spam recém-programada. O tempo pode ser definido pela repetição da execução da atualização do Anti-Spam depois de um determinado período (***Executar a cada...***), pela definição de uma data e hora exatas (***Executar na hora específica***) ou pela definição de um evento ao qual a execução da atualização deve ser associada (***Ação baseada na inicialização do computador***).

Opções avançadas de programação

Esta seção permite definir sob quais condições a atualização do Anti-Spam deverá ou não ser executada se o computador estiver no modo de pouca energia ou completamente desligado.

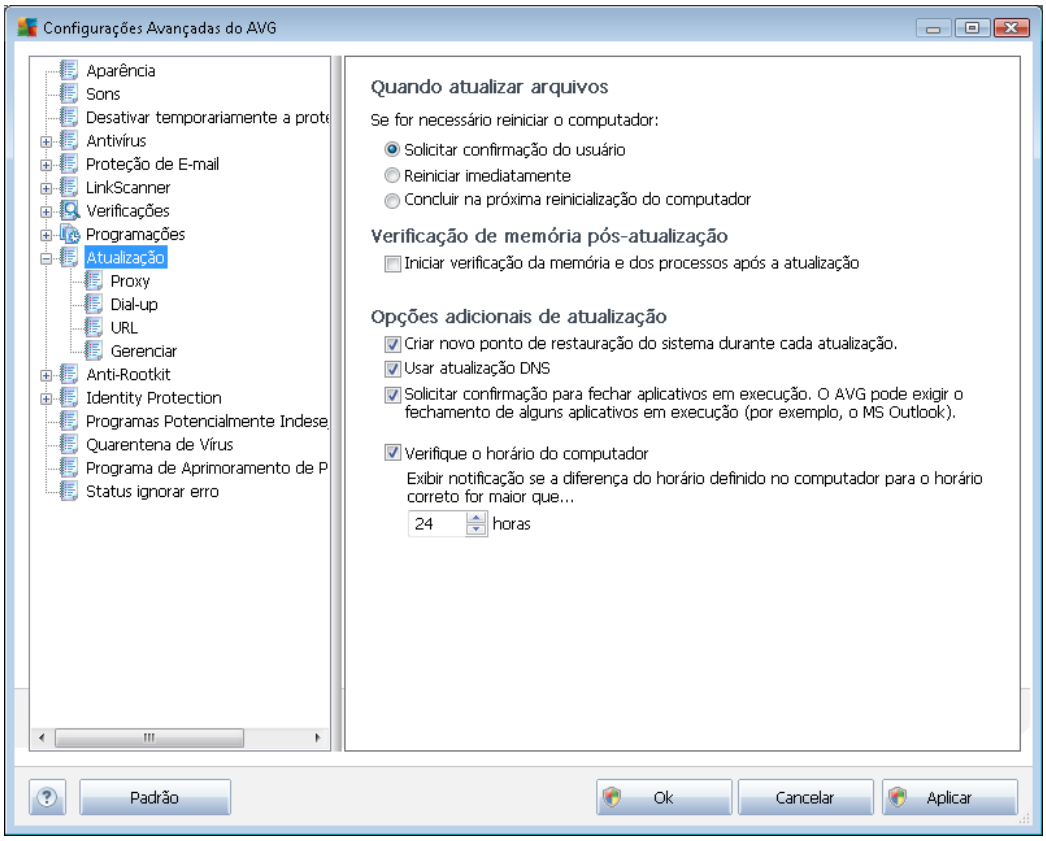
Outras configurações de atualização

Marque a opção ***Executar novamente a atualização assim que uma conexão com a Internet estiver disponível*** para ter certeza de que, se a conexão com a Internet for corrompida e o processo de atualização do Anti-Spam falhar, ele será imediatamente reiniciado quando a conexão com a Internet for restaurada.

Assim que a verificação agendada for iniciada na hora especificada, você será informado por uma janela pop-up aberta sobre o ícone AVG na bandeja do sistema (*caso você tenha mantido a configuração padrão da caixa de diálogo Configurações avançadas/Aparência).*

9.9. Atualizar

O item de navegação ***Atualizar*** abre uma nova caixa de diálogo na qual é possível especificar parâmetros gerais relativos à atualização do AVG:



Quando atualizar arquivos

Nesta seção você poderá escolher entre três opções alternativas caso o processo de atualização requeira a reinicialização do PC. A finalização da atualização pode ser agendada para a próxima reinicialização do PC, ou você pode reiniciar imediatamente:

- ***Requer a confirmação do usuário*** *(por padrão)* - será solicitado que você aprove a reinicialização do PC necessária para finalizar o processo de atualização

- ***Reiniciar imediatamente*** - o computador será reiniciado automaticamente após a conclusão do processo de atualização, e sua aprovação não será necessária.

- ***Concluir na próxima reinicialização do computador*** - a finalização do processo de atualização será adiada até a próxima reinicialização do computador. Lembre que esta opção só é recomendada se você tiver certeza que o computador é reinicializado regularmente, pelo menos uma vez por dia!

Verificação de memória pós-atualização

Marque essa caixa de seleção para definir que deseja iniciar uma nova verificação de memória depois de cada atualização concluída com êxito. A atualização mais atual baixada pode conter novas definições de vírus, e estas devem ser aplicadas à verificação imediatamente.

Opções adicionais de atualização

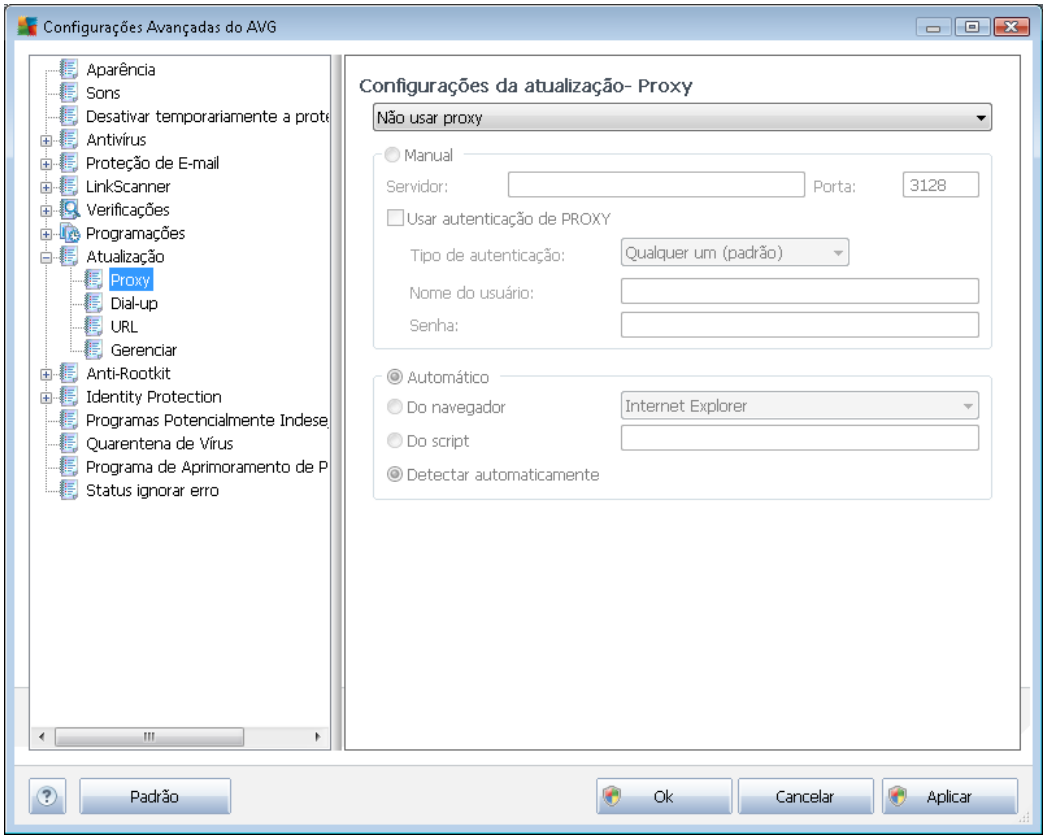
- ***Criar novo ponto de restauração do sistema durante cada atualização do programa*** - antes de cada ativação da atualização do programa AVG, um ponto de restauração do sistema é criado. No caso de falha no processo de atualização e seu sistema operacional, você pode restaurar o seu SO para a configuração original deste ponto. Esta opção está disponível em Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauração do Sistema, mas quaisquer alterações podem ser recomendadas apenas para usuários experientes! Mantenha esta caixa de seleção marcada se quiser usar o recurso.

- ***Usar atualização DNS*** (*ativada por padrão*) - com este item marcado, depois que a atualização é iniciada, o **AVG Internet Security 2012** procura informações sobre a mais recente versão do banco de dados de vírus e sobre a versão mais recente do programa no servidor DNS. Então, somente os menores e mais indispensáveis arquivos de atualização são baixados e aplicados. Dessa forma, a quantidade total de dados baixados é reduzida e o processo de atualização é executado mais rapidamente.

- ***Requer confirmação para fechar aplicativos em execução*** (*ativado por padrão*) ajudará você a se certificar de que nenhum aplicativo em execução no momento será fechado sem sua permissão - se necessário para a conclusão do processo de atualização.

- ***Marcar o horário definido do computador*** - marque esta opção para declarar que você deseja que seja exibida uma notificação caso o horário do computador seja diferente do horário correto em um número de horas maior que o especificado.

9.9.1. Proxy



O servidor proxy é um servidor autônomo ou um serviço executado em um PC que garante conexão segura à Internet. De acordo com as regras de rede especificadas, você poderá acessar a Internet diretamente ou por meio do servidor proxy; as duas possibilidades também podem ser permitidas ao mesmo tempo. Em seguida, no primeiro item da caixa de diálogo ***Configurações da Atualização - Proxy*** , você deverá selecionar o menu da caixa de combinação, se desejar:

- ***Usar proxy***
- ***Não usar proxy*** - configuração padrão
- ***Tentar conectar usando proxy e, se falhar, conectar diretamente***

Se você selecionar uma opção usando o servidor proxy, terá que especificar alguns outros dados. As configurações do servidor podem ser definidas manualmente ou automaticamente.

Configuração manual

Se você selecionar a configuração manual (selecione a opção *Manual* ***para ativar a seção apropriada da caixa de diálogo***), terá que especificar os seguintes itens:

- ***Servidor*** – especifique o endereço IP do servidor ou o nome do servidor.

- ***Porta*** - especifique o número da porta que permite o acesso à Internet (*por padrão, esse número está definido como 3128, mas pode ser definido de forma diferente - se não tiver certeza, entre em contato com o administrador da rede*).

O servidor proxy também pode ter configurado regras especificas para cada usuário. Se o servidor proxy estiver configurado dessa forma, selecione a opção ***Usar autenticação PROXY*** para verificar se o nome de usuário e a senha são válidos para conexão à Internet por meio do servidor proxy.

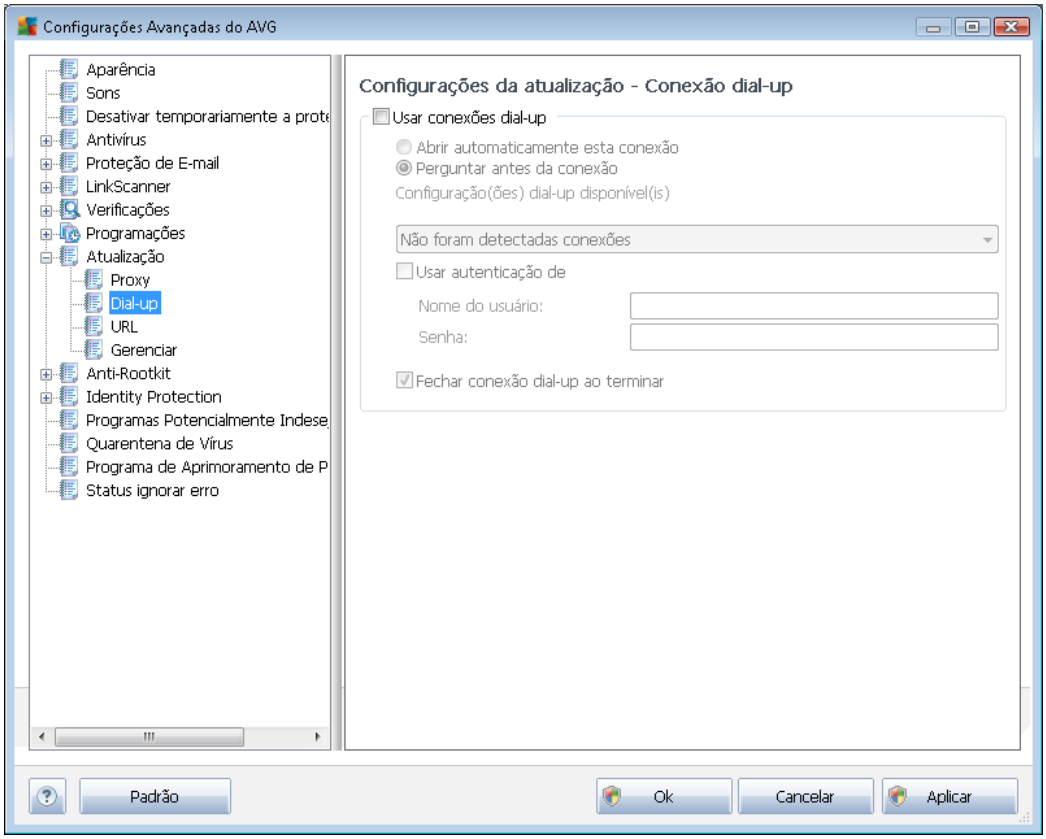
Configuração automática

Se você selecionar configuração automática (*marque a opção Automática* ***para ativar a seção da caixa de diálogo apropriada***), selecione de onde a configuração do proxy deve ser realizada:

- ***A partir do navegador*** - a configuração será lida a partir do navegador da Internet padrão
- ***Do script*** - a configuração será lida de um script de download com a função retornando o endereço proxy
- ***Detecção automática*** - a configuração será detectada de forma automática e direta do servidor proxy

9.9.2. Dial-up

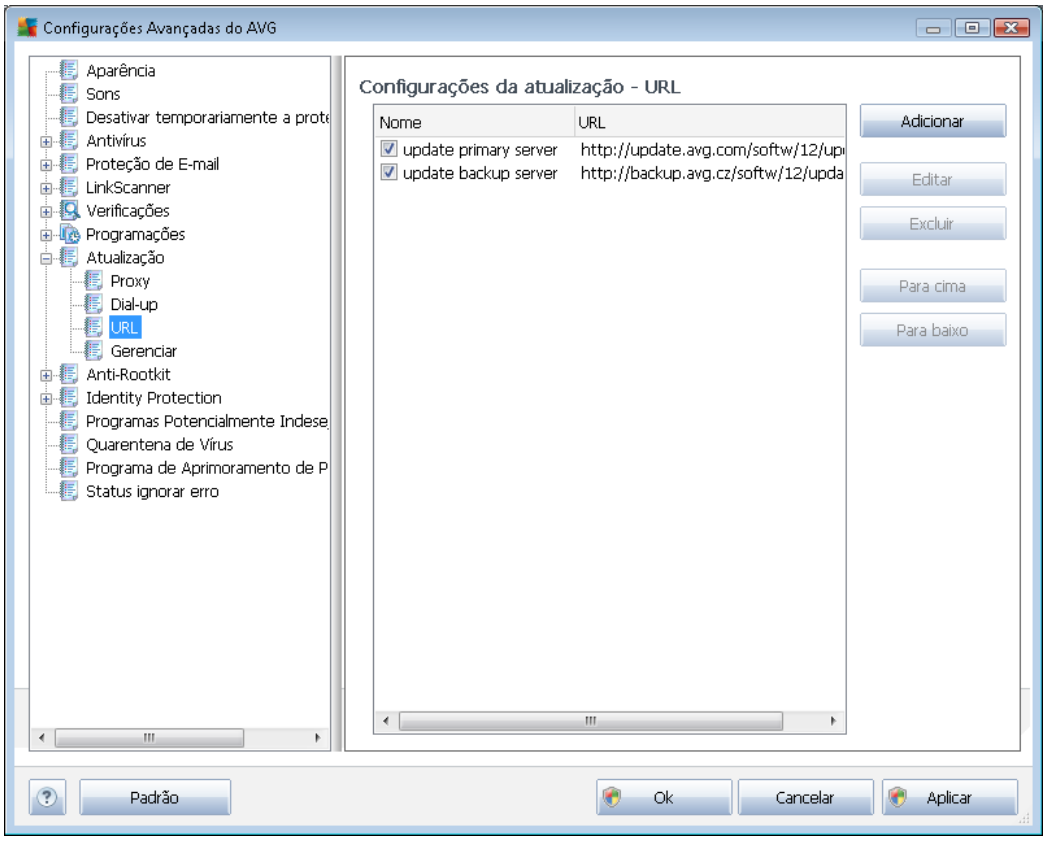
Todos os parâmetros definidos opcionalmente na caixa de diálogo ***Atualizar configurações - Conexão dial-up*** referem-se à conexão discada com a Internet. Os campos da guia estarão inativos até que a opção ***Usar conexões dial-up***, que ativará os campos, esteja marcada:



Especifique se você deseja se conectar à Internet automaticamente (***Abrir esta conexão automaticamente***) ou se deseja confirmar a conexão manualmente, todas as vezes (***Perguntar antes da conexão***). Para conexão automática, você poderá decidir se a conexão deve ser fechada após o término da atualização (***Fechar conexão dial-up ao terminar***).

9.9.3. URL

A caixa de diálogo ***URL*** oferece uma lista de endereços da Internet, a partir da qual você poderá baixar os arquivos de atualização:



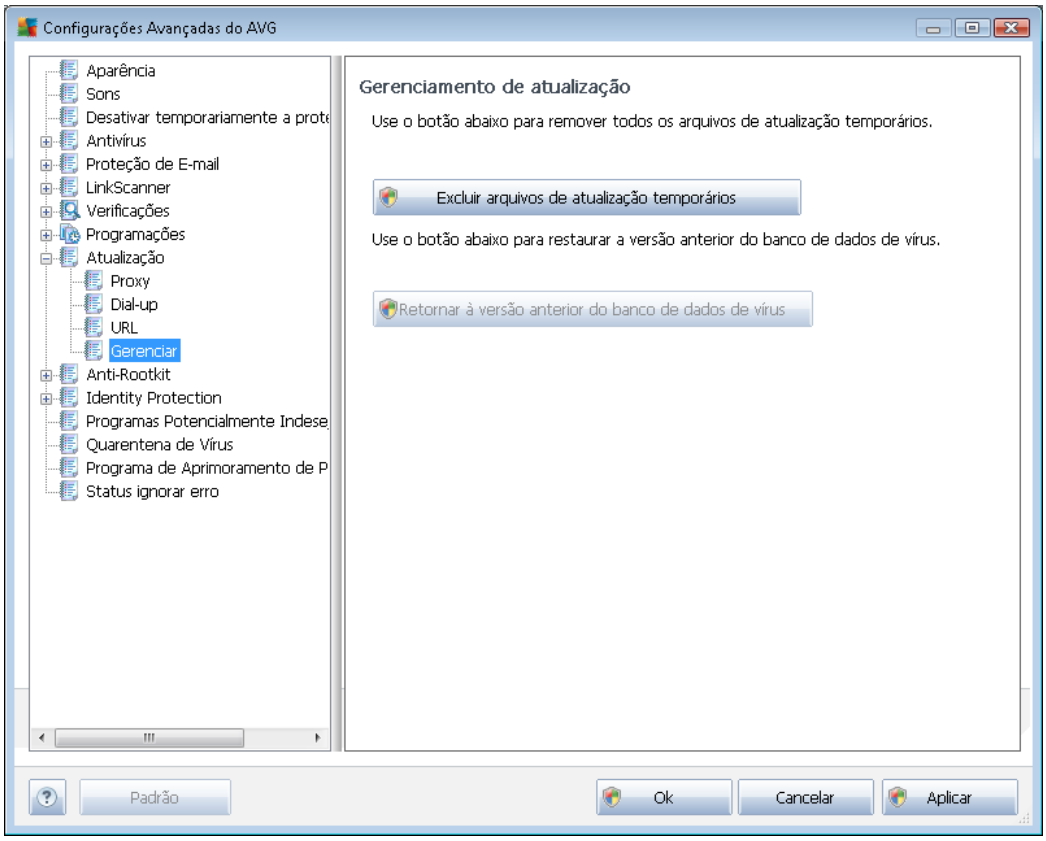
Botões de controle

A lista e os itens podem ser modificados por meio dos seguintes botões de controle:

- ***Adicionar***- abre uma caixa de diálogo na qual você especificará a nova URL a ser adicionada à lista
- ***Editar*** – abre uma caixa de diálogo na qual você poderá editar os parâmetros da URL selecionada
- ***Excluir*** - exclui a URL selecionada da lista
- ***Mover para Cima*** -move a URL selecionada uma posição acima na lista
- ***Mover para Baixo*** – move a URL selecionada uma posição abaixo na lista.

9.9.4. Gerenciar

A caixa de diálogo ***Gerenciamento de atualização*** oferece duas opções que podem ser acessadas por meio de dois botões:

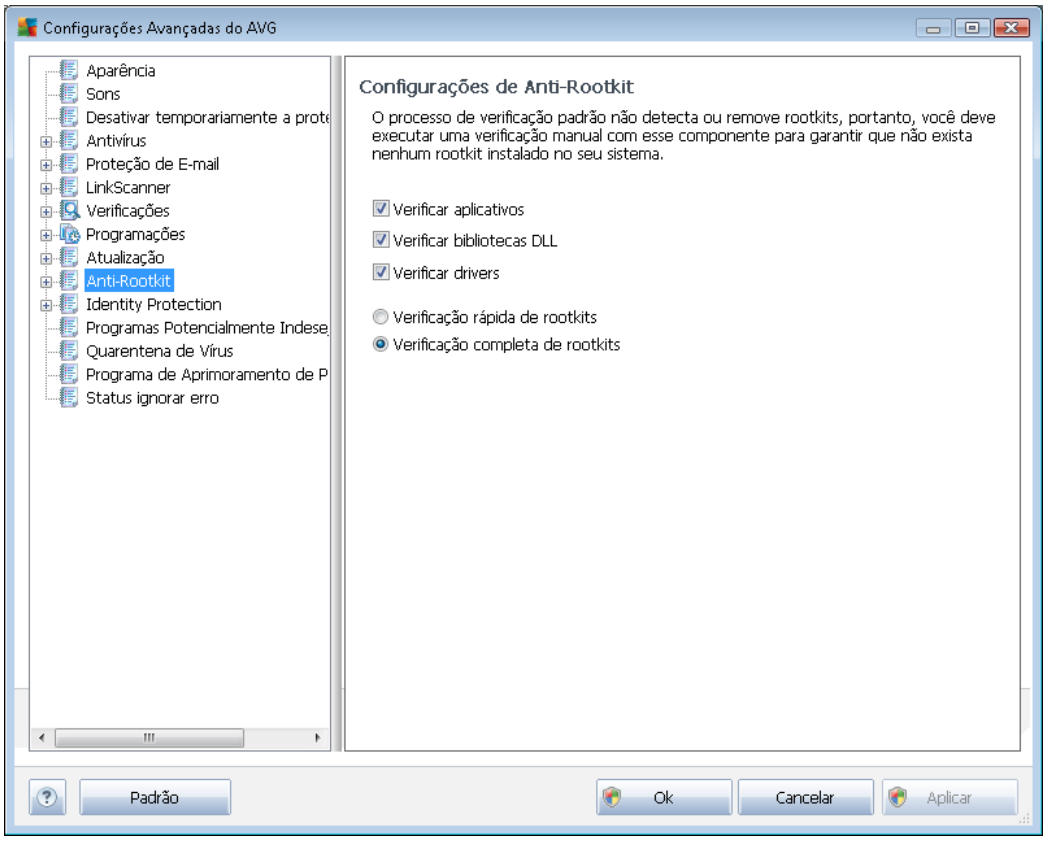


- ***Excluir arquivos de atualização temporários*** - pressione este botão para excluir todos os arquivos de atualização redundantes do seu disco rígido (*por padrão, eles são armazenados por 30 dias*)

- ***Retornar banco de dados de vírus para a versão anterior*** –pressione este botão para excluir a versão mais recente da base de vírus do seu disco rígido e retornar à versão salva anteriormente (*a nova versão da base de vírus fará parte da próxima atualização*)

9.10. Anti-Rootkit

Na caixa de diálogo ***Configurações de Anti-Rootkit***, você pode editar a configuração do componente Anti-Rootkit:



A edição de todas as funções do componente Anti-Rootkit, conforme fornecida por esta caixa de diálogo, também pode ser acessada diretamente na interface do componente Anti-Rootkit.

Marque as respectivas caixas de seleção para especificar objetos que devem ser verificados:

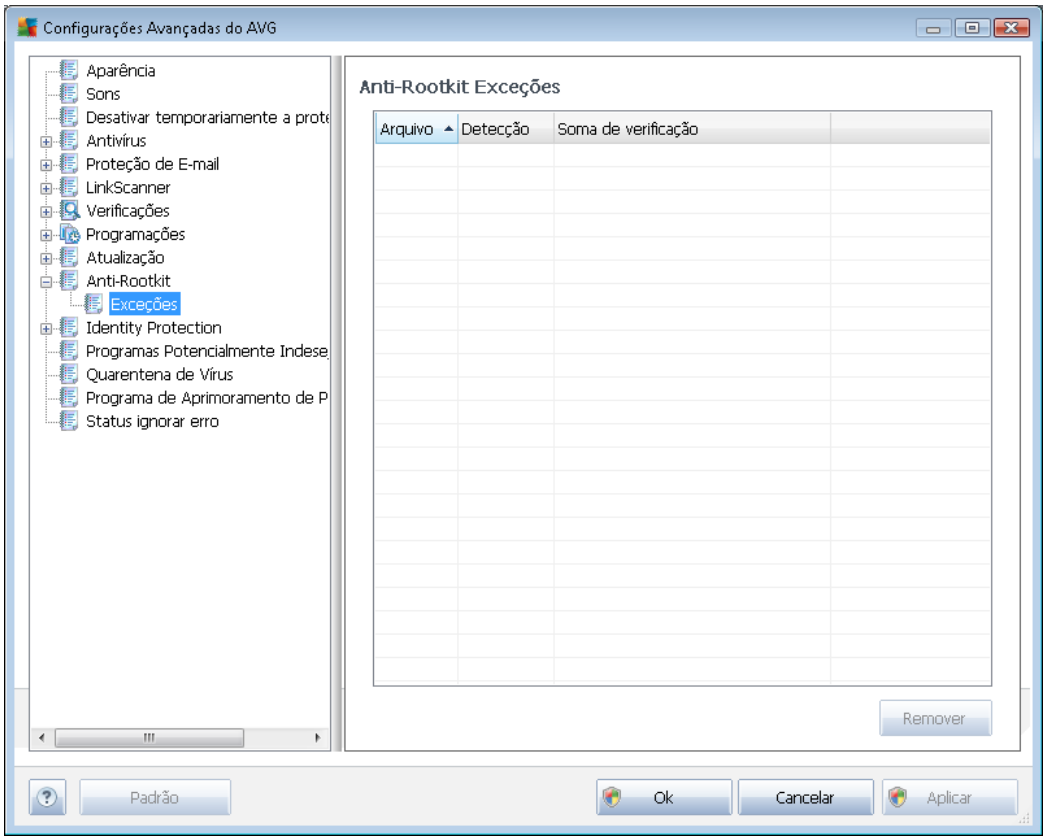
- ***Verificar aplicativos***
- ***Verificar bibliotecas DLL***
- ***Verificar drivers***

Em seguida, você pode selecionar o modo de verificação do rootkit:

- ***Verificação rápida do rootkit*** - verifica todos os processos em execução, unidades carregadas e pasta do sistema (*tipicamente c:\Windows*)
- ***Verificação completa do rootkit*** - verifica todos os processos em execução, unidades carregadas, a pasta do sistema (*tipicamente c:\Windows*além de todos os discos locais (*incluindo o disco flash, mas excluindo as unidades de CD/disquete*)

9.10.1. Exceções

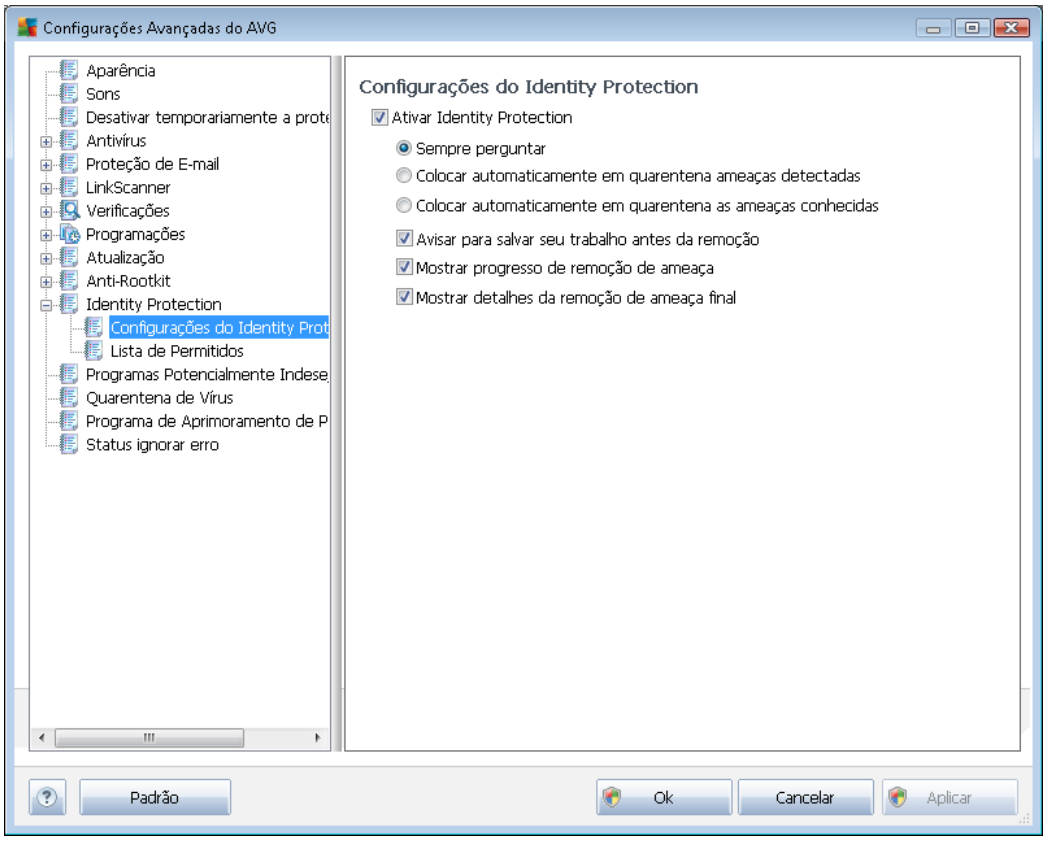
Na caixa de diálogo ***Exceções de Anti-Rootkit***, você pode definir os arquivos específicos *(por exemplo, alguns drivers que possam ser detectados como rootkits erroneamente)* que devem ser excluídos da verificação:



9.11. Identity Protection

9.11.1. Configurações do Identity Protection

A caixa de diálogo ***Configurações do Identity Protection***permite ativar/desativar os recursos elementares do componente Identity Protection:



Ativar Identity Protection (*ativada por padrão*) – desmarque para desativar o componente Identity Protection.

É altamente recomendável não fazer isso a menos que você precise!

Quando o Identity Protection está ativado, você pode especificar o que fazer quando uma ameaça é detectada:

- ***Perguntar sempre*** (*ativado por padrão*) - quando uma ameaça for detectada, será perguntado se deseja movê-la para a quarentena para assegurar que aplicativos que você deseja executar não sejam removidos.
- ***Colocar ameaças detectadas automaticamente em quarentena*** - marque essa caixa para definir que deseja mover todas as ameaças possivelmente detectadas para um espaço seguro da Quarentena de Vírus do imediatamente. Se você mantiver as configurações padrão, quando uma ameaça for detectada, será perguntado se você deseja movê-la para a quarentena para assegurar que aplicativos que você deseja executar não sejam removidos.
- ***Colocar automaticamente em quarentena as ameaças detectadas*** - marque esse item

se desejar que todos os aplicativos detectados como possíveis malware sejam movidos automaticamente e imediatamente para a Quarentena de Vírus do.

Posteriormente você pode atribuir itens específicos para ativar de modo opcional mais recursos do Identity Protection:

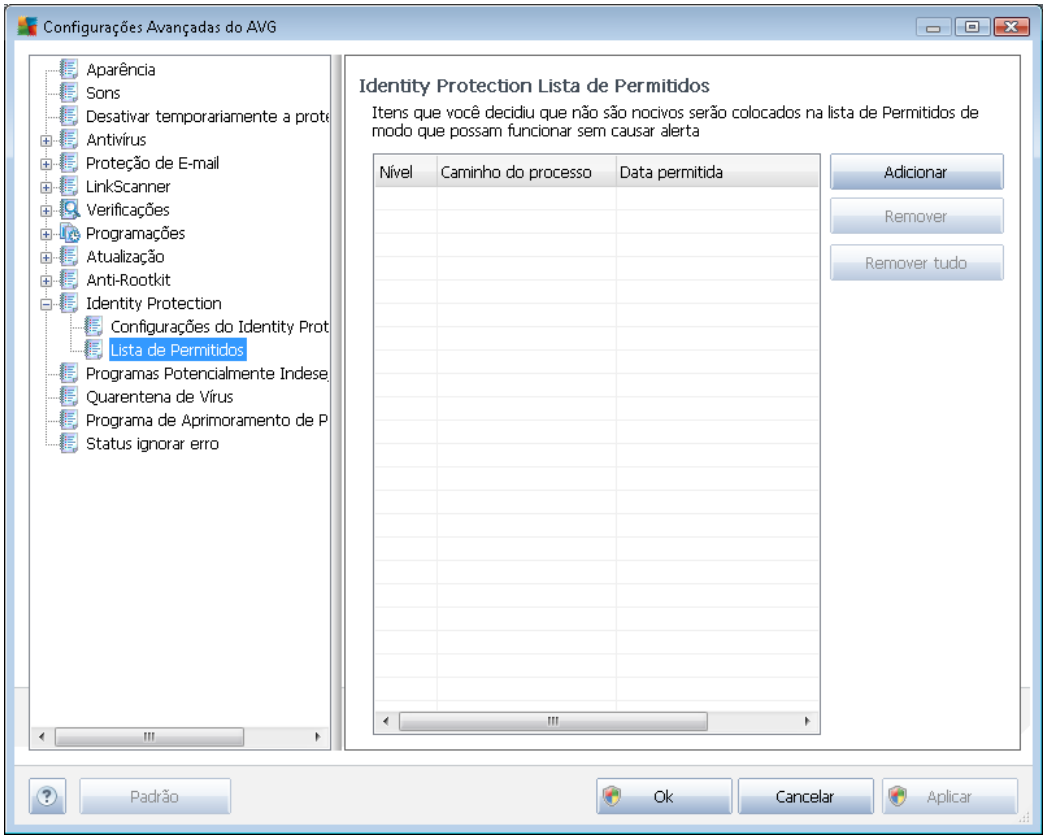
- ***Solicitar salvar o trabalho antes da remoção*** - (*ativado por padrão*) - marque esse item se desejar se avisado antes do aplicativo detectado como possível malware ser removido para quarentena. Caso você esteja trabalhando com o aplicativo, seu projeto poderá ser perdido e você deverá salvá-lo antes. Por padrão, este item está ativado e recomendamos fortemente mantê-lo assim.

- ***Exibir progresso de remoção de malware*** - (*somente por padrão*) - com esse item ativado, quando um malware potencial é detectado, uma nova caixa de diálogo é aberta para exibir o andamento do malware movido para quarentena.

- ***Exibir detalhes finais de remoção de malware*** - (*ativado por padrão*) - com esse item ativado, o Identity Protection exibe informações detalhadas sobre cada objeto movido para quarentena (*nível de gravidade, localização etc).*).

9.11.2. Lista de permissões

Na caixa de diálogo ***Configurações do Identity Protection***, se você optar por manter o item ***Colocar automaticamente em quarentena ameaças detectadas*** desmarcado, sempre que um malware perigoso for detectado, será perguntado se você deseja removê-lo. Se depois você atribuir o aplicativo suspeito (*detectado com base em seu comportamento*) como seguro e confirmar que ele deve ser mantido no computador, o aplicativo será adicionado à chamada ***Identity Protection - Lista de permitidos*** e não será mais reportado como perigoso:



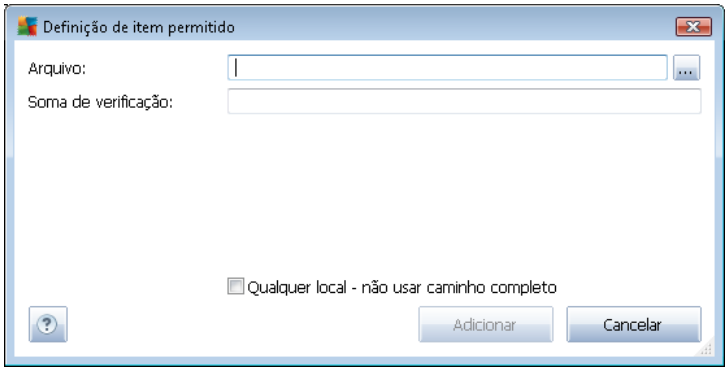
A ***Identity Protection - Lista de permitidos*** fornece as seguintes informações sobre cada aplicativo:

- ***Nível*** - identificação gráfica da respectiva severidade do processo em uma escala de quatro níveis, variando do menos importante (□□□□) até o mais crítico (■■■■)
- ***Caminho do processo*** - caminho para o local do arquivo executável do aplicativo (*processo*)
- ***Data da permissão*** - data na qual você atribuiu manualmente o aplicativo como seguro

Botões de controle

Os botões de controle disponíveis na caixa de diálogo ***Lista de permissão do Identity Protection*** são os seguintes:

- ***Adicionar*** - pressione esse botão para adicionar um novo aplicativo à lista de permissões. A caixa de diálogo a seguir é ativada:

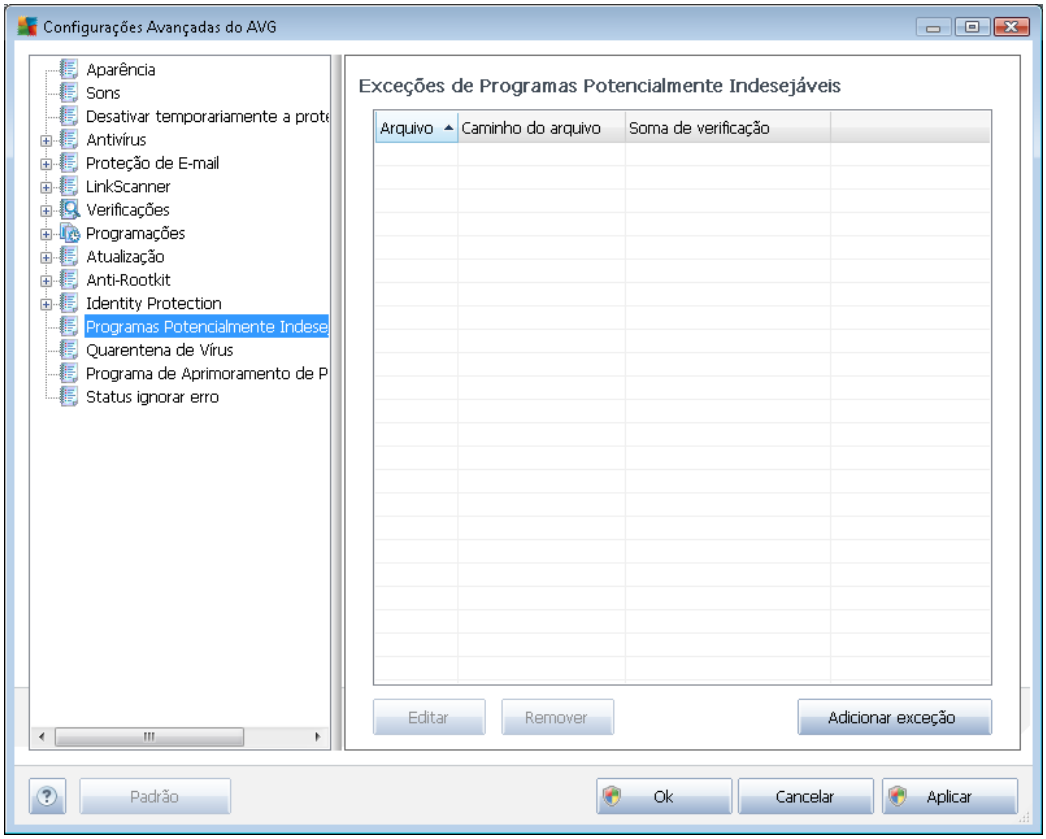


- ***Arquivo -*** digite o caminho completo para o arquivo (*aplicativo*) que você deseja marcar como exceção
- ***Soma de Verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo escolhido dos outros arquivos. A Soma de verificação é gerada e exibida após a adição bem-sucedida do arquivo.
- Qualquer local - não use caminhos completos - se quiser definir o arquivo como uma exceção apenas no local específico, deixe a caixa de seleção desmarcada

- ***Remover*** - pressione para remover o aplicativo selecionado da lista
- ***Remover tudo*** - pressione para remover todos os aplicativos listados

9.12. Programas Potencialmente Indesejáveis

O AVG Internet Security 2012 é capaz de analisar e detectar aplicativos executáveis ou bibliotecas DLL que possam ser potencialmente indesejáveis no sistema. Pode ser que o usuário deseje manter, em alguns casos, determinados programas indesejáveis no computador (programas instalados propositalmente). Alguns programas, especialmente os gratuitos, incluem adware. Esse tipo de adware pode ser detectado e informado pelo **AVG Internet Security 2012** como um *programa potencialmente indesejável*. Se desejar manter esse programa no computador, você poderá defini-lo como uma exceção de programa potencialmente indesejável:

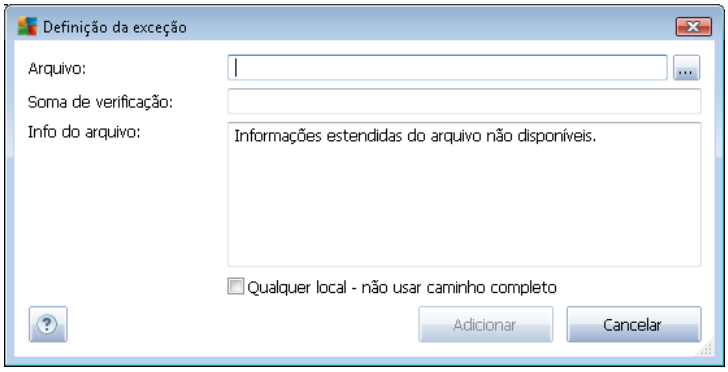


A caixa de diálogo ***Exceções de programa potencialmente indesejável*** exibe uma lista das exceções definidas e válidas atualmente dos programas não desejados. É possível editar a lista, excluir itens existentes ou adicionar novas exceções. As informações a seguir podem ser encontradas na lista para cada exceção:

- ***Arquivo*** - fornece o nome exato do respectivo aplicativo
- ***Caminho do arquivo*** - mostra a localização do aplicativo
- ***Soma de Verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo escolhido dos outros arquivos. A Soma de verificação é gerada e exibida após a adição bem-sucedida do arquivo.

Botões de controle

- ***Editar*** - abre uma caixa de diálogo de edição (*idêntica à da definição de exceção; veja abaixo*) de uma exceção já definida, na qual é possível alterar os parâmetros de exceção
- ***Remover*** - exclui o item selecionado da lista de exceções
- ***Adicionar exceção*** - abre uma caixa de diálogo de exceção na qual é possível definir os parâmetros da nova exceção a ser criada:



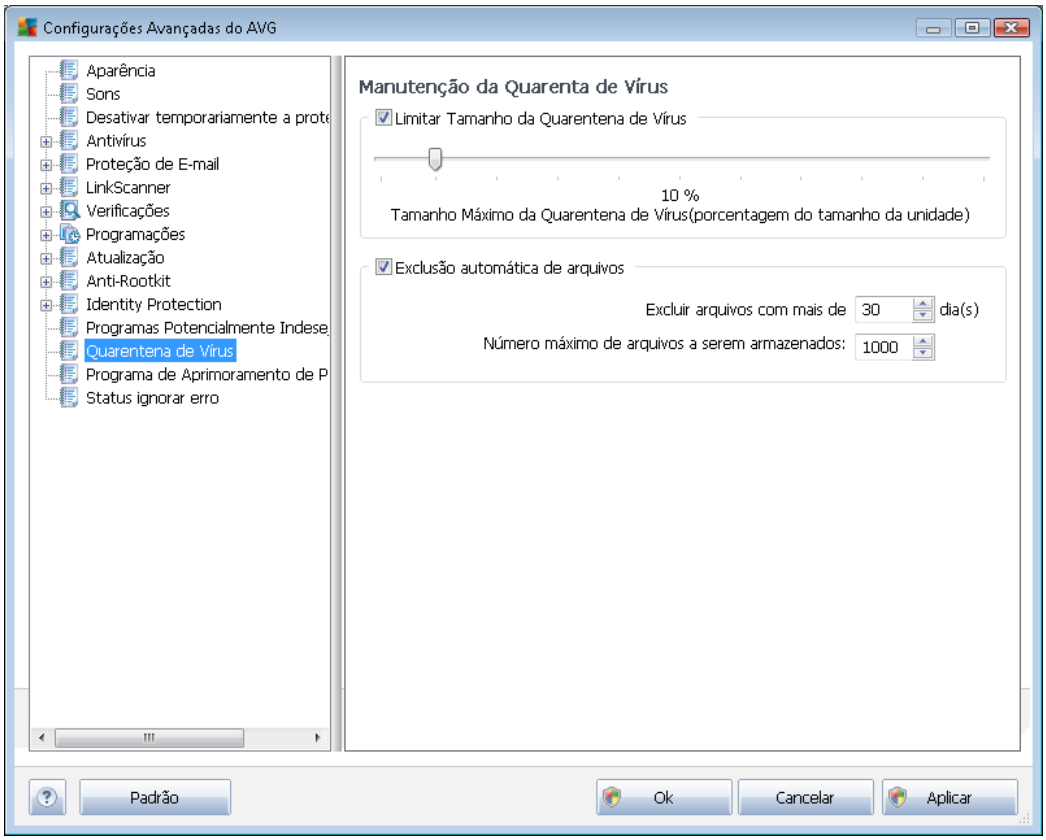
- ***Arquivo*** - digite o caminho completo para o arquivo que deseja marcar como uma exceção

- ***Soma de verificação*** - exibe a 'assinatura' exclusiva do arquivo selecionado. Essa Soma de verificação é uma string de caracteres gerados automaticamente, que permite ao AVG diferenciar inequivocamente o arquivo escolhido dos outros arquivos. A Soma de verificação é gerada e exibida após a adição bem-sucedida do arquivo.

- ***Informações do Arquivo*** - exibe outras informações disponíveis sobre o arquivo *(informações de licença/versão etc.)*

- ***Qualquer local - não use caminhos completos*** - se quiser definir o arquivo como uma exceção apenas no local específico, deixe a caixa de seleção desmarcada. Se a caixa de seleção estiver marcada, o arquivo especificado será definido como uma exceção, não importa onde esteja. *Entretanto, você precisa especificar o caminho completo para o arquivo específico de qualquer forma. O arquivo será usado como um exemplo exclusivo para a possibilidade de que dois arquivos com o mesmo nome apareçam no sistema*.

9.13. Quarentena de vírus



A caixa de diálogo ***Manutenção da quarentena*** permite definir vários parâmetros relativos à administração de objetos armazenados na Quarentena:

- ***Limitar tamanho da Quarentena de vírus*** - use o controle deslizante para definir o tamanho máximo da Quarentena de vírus. O tamanho é especificado proporcionalmente ao tamanho do seu disco rígido local.

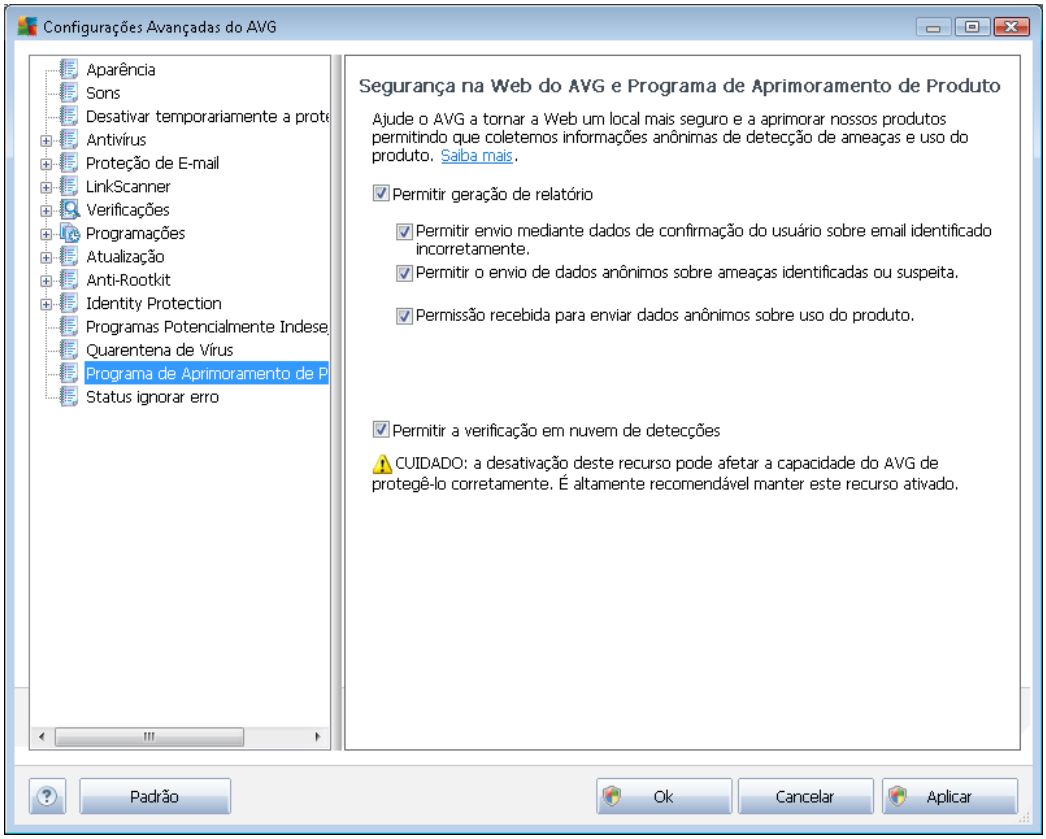
- ***Exclusão automática de arquivo*** - nesta seção, defina a duração máxima de armazenamento dos objetos na Quarentena (***Excluir arquivos mais antigos que...***) e o número máximo de arquivos a serem armazenados na Quarentena (***Número máximo de arquivos a serem armazenados***).

9.14. Programa de aprimoramento de produtos

A caixa de diálogo ***Segurança na Web e Programa de Aprimoramento de Produto*** convida você a participar do aperfeiçoamento do produto AVG e nos ajudar a aumentar o nível de segurança geral na Internet. Mantenha a opção ***Permitir relatórios*** marcada, a fim de permitir que sejam gerados relatórios de ameaças detectadas para os laboratórios da AVG. Isso nos ajuda a coletar informações atualizadas sobre as ameaças mais recentes dos participantes do mundo todo e, em retorno, podemos melhorar a proteção para todos.

O relatório é feito automaticamente, evitando inconvenientes. Nenhum dado pessoal é

incluído nos relatórios. A geração de relatórios de ameaças detectadas é opcional. No entanto, solicitamos que você mantenha essa opção ativada. Ela nos ajuda a melhorar a proteção para você e para os usuários do AVG.



Hoje em dia, existem muito mais ameaças do que apenas vírus comuns. Os criadores de códigos maliciosos e sites perigosos são muito inovadores, e novos tipos de ameaças surgem frequentemente, a vasta maioria na Internet. Estas são algumas das mais comuns:

- ***Um vírus*** é um código mal-intencionado que se copia e se espalha, muitas vezes sem ser percebido, até que o estrago seja feito. Alguns vírus são uma ameaça séria, excluindo ou alterando deliberadamente arquivos no seu caminho, enquanto alguns vírus podem fazer algo aparentemente inofensivo, como reproduzir o trecho de uma música. No entanto, todos os vírus são perigosos devido à capacidade básica de se multiplicarem – mesmo um vírus simples pode ocupar toda a memória do computador em um instante e causar uma falha.

- ***O worm*** é uma subcategoria de vírus que, diferentemente de um vírus normal, não precisa de um objeto "transportador" ao qual se anexar. Ele se envia a outros computadores dentro de si mesmo, normalmente por e-mail e, como resultado, frequentemente sobrecarrega servidores de e-mail e sistemas de rede.

- ***O spyware normalmente é definido como uma categoria de malware (malware = qualquer software mal intencionado, incluindo vírus) que abrange programas – tipicamente Cavalos de Tróia – com o objetivo de roubar informações pessoais,***

senhas, números de cartão de crédito ou para se infiltrar em um computador e permitir que o atacante controle-o remotamente; é claro que tudo isso sem o conhecimento ou consentimento do dono do computador.

- ***Programas potencialmente indesejados*** são um tipo de spyware que pode ser, mas não necessariamente precisa ser, perigoso ao computador. Um exemplo específico de um PPI é o adware, software projetado para distribuir propaganda, normalmente exibindo pop-ups de anúncio; é irritante, mas não diretamente prejudicial.

- ***Os cookies de rastreamento*** podem também ser contados como um tipo de spyware, uma vez que esses pequenos arquivos, armazenados no navegador da Web e enviados automaticamente ao site "pai" quando você visitá-lo novamente, podem conter dados como seu histórico de navegação e outras informações similares.

- ***Vulnerabilidade*** é um código mal intencionado que se aproveita de uma falha ou vulnerabilidade em um sistema operacional, navegador da Internet ou outro programa essencial.

- ***Phishing*** é uma tentativa de adquirir dados pessoais confidenciais simulando uma organização confiável e bem conhecida. Normalmente, as possíveis vítimas são contatadas por um e-mail em massa solicitando que elas, por exemplo, atualizem os detalhes da sua conta bancária. Para fazer isso, elas são convidadas a seguir o link fornecido que leva a um site falso do banco.

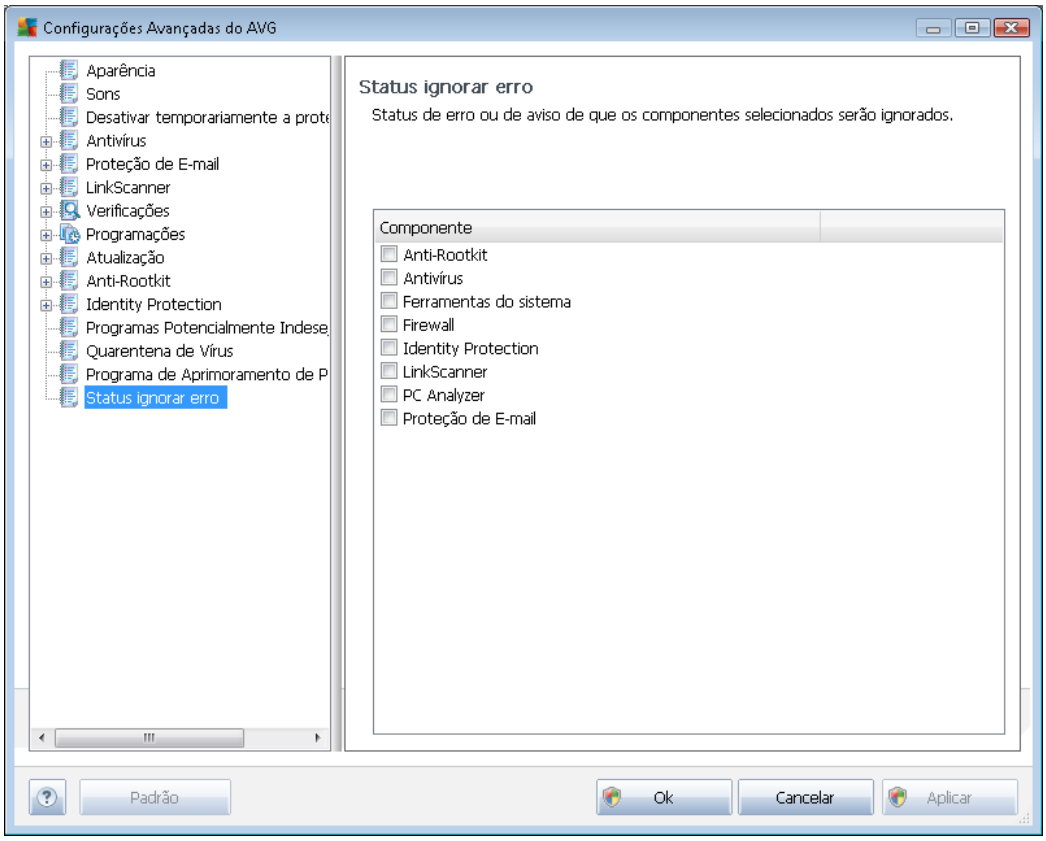
- ***Hoax é um e-mail em massa contendo informações perigosas, alarmantes ou apenas irritantes e inúteis.*** Muitas das ameaças acima usam o e-mail hoax para se espalharem.

- ***Sites mal-intencionados*** são aqueles que deliberadamente instalam software mal-intencionado no seu computador, e sites invadidos fazem o mesmo, a única diferença é que esses sites são legítimos, foram invadidos e infectam os visitantes.

Para protegê-lo de todos esses diferentes tipos de ameaças, o AVG Internet Security 2012 inclui componentes especializados. Para obter uma breve descrição desses componentes, consulte o capítulo Visão geral dos componentes.

9.15. Status ignorar erro

Na caixa de diálogo ***Ignorar status de erro*** você pode selecionar os componentes dos quais não deseja receber informações:



Por padrão, não há componentes selecionados nesta lista. Isto significa que, caso qualquer componente receba um status de erro, você será informado sobre isso imediatamente via:

- ícone da bandeja do sistema - enquanto todos os componentes do AVG estão funcionando adequadamente, o ícone é exibido em quatro cores; entretanto, se ocorrer um erro, os ícones aparecem com um ponto de exclamação amarelo,
- descrição textual do problema na seção Informações sobre Status de Segurança na janela principal do AVG

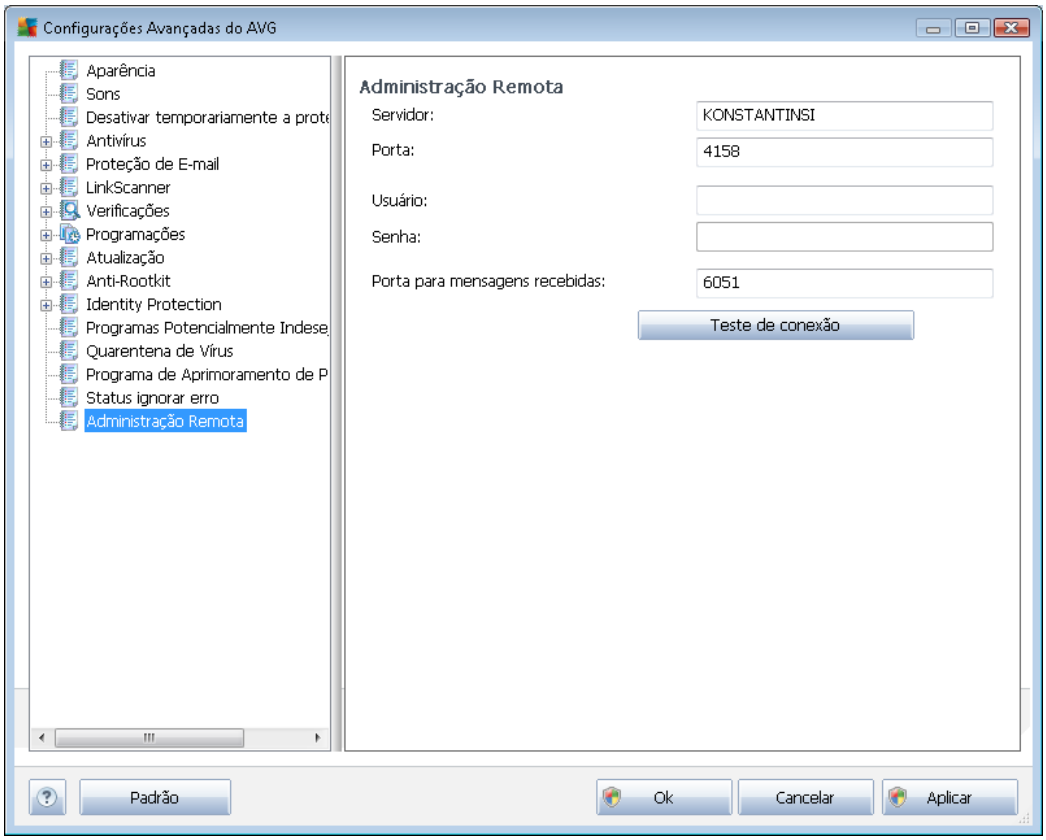
Pode acontecer que, por alguma razão, você precise desligar um componente por certo tempo (*não é recomendável, você deve tentar manter todos os componentes sempre ligados e em sua configuração padrão, mas pode acontecer*). Neste caso, o ícone da bandeja do sistema relata automaticamente o status de erro do componente. Entretanto, neste caso em particular, não se pode falar de um erro, pois você deliberadamente o induziu, e está ciente do provável risco. Ao mesmo tempo, assim que é exibido em cinza, o ícone não pode relatar qualquer outro erro que possa aparecer.

Neste caso, na caixa de diálogo acima você pode selecionar componentes que podem estar com

status de erro (*ou desligados*) e sobre os quais você não deseja receber informações. A mesma opção *(Ignorar estado do componente* também está disponível para componentes específicos diretamente da visão geral dos componentes na janela principal do AVG.

9.16. Administração Remota

O item ***Administração Remota*** e a caixa de diálogo respectiva serão exibidas na árvore de navegação somente se você tiver instalado seu **AVG Internet Security 2012** com uma licença do AVG Business Edition e se, durante o processo de instalação, você tiver confirmado que deseja instalar o componente ***Administração Remota***. Para obter uma descrição detalhada da instalação e configuração da administração remota, consulte a documentação respectiva do AVG Network Edition, que está disponível para download no site do AVG (http://www.avg.com/), na seção Centro de suporte/Download.



A configuração ***Administração Remota*** se refere à conexão da estação do cliente AVG com o sistema de administração remota. Se você planeja conectar a estação apropriada à administração remota, especifique os seguintes parâmetros:

- ***Servidor*** - nome do servidor (ou endereço IP do servidor) em que o AVG Admin Server está instalado
- ***Porta*** - fornece o número da porta em que o cliente do AVG se comunica com o AVG Admin Server (*o número da porta 4158 é considerado padrão. Se você usá-lo, não terá que especificá-lo explicitamente*)

- ***Login*** - se a comunicação entre o cliente AVG e o AVG Admin Server for definida como segura, forneça o nome de usuário ...
- ***Senha*** - ... e a senha
- ***Porta para mensagens recebidas*** - número da porta em que o cliente AVG aceita mensagens recebidas do AVG Admin Server

Botões de controle

O botão ***Testar conexão*** ajuda a verificar se todos os dados mencionados acima são válidos e podem ser usados para uma conexão bem-sucedida com o DataCenter.

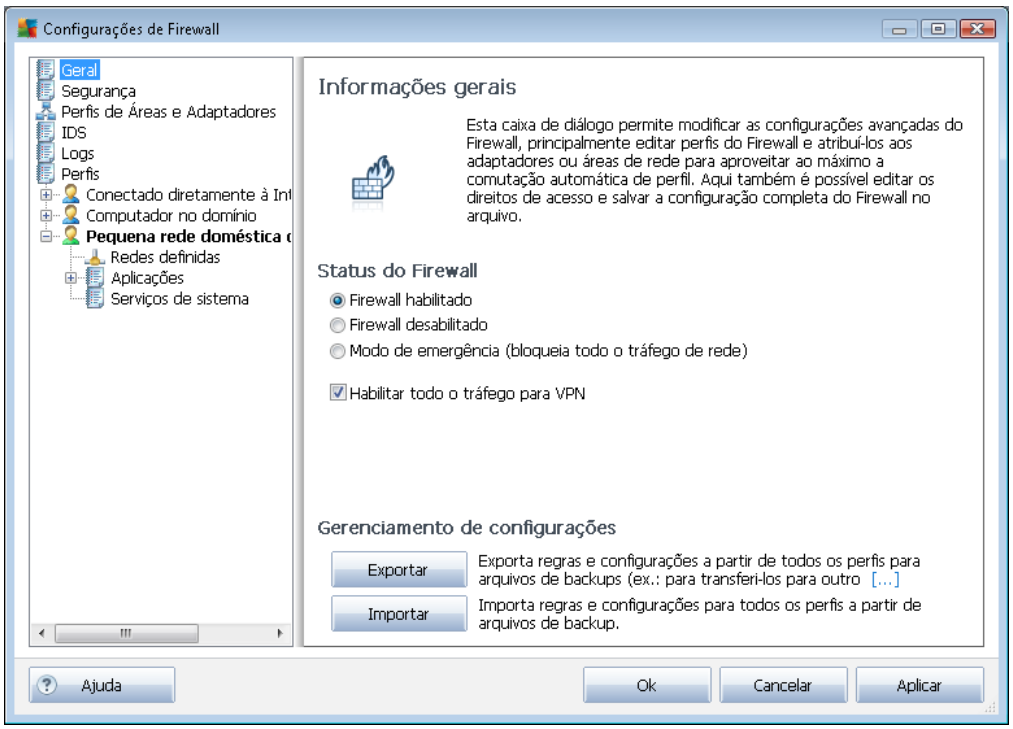
10. Configurações de Firewall

A configuração do Firewall é aberta em uma nova janela com várias caixas de diálogo para configuração de parâmetros avançados do componente.

No entanto, o fornecedor do software configurou todos os componentes do AVG Internet Security 2012 para proporcionar um desempenho ideal. A menos que você tenha um motivo real para isso, não altere as configurações padrão. As alterações nas configurações devem ser feitas somente por um usuário experiente.

10.1. Geral

A caixa de diálogo ***Informações gerais*** está dividida em duas seções:



Status do Firewall

Na seção ***Status do firewall***, você pode trocar o status do Firewall de acordo com a necessidade:

- ***Firewall ativado -*** selecione esta opção para permitir a comunicação nesses aplicativos considerados 'permitidos' no conjunto de regras definidas no perfil de Firewall selecionado.
- ***Firewall desativado -*** esta opção desativa totalmente o Firewall, todo o tráfego da rede é permitido mas não verificado!
- ***Modo de emergência (bloquear todo o tráfego de Internet)*** - selecione esta opção para bloquear todo o tráfego em cada porta de rede; o Firewall ainda está em execução, mas

todo o tráfego da rede foi interrompido.

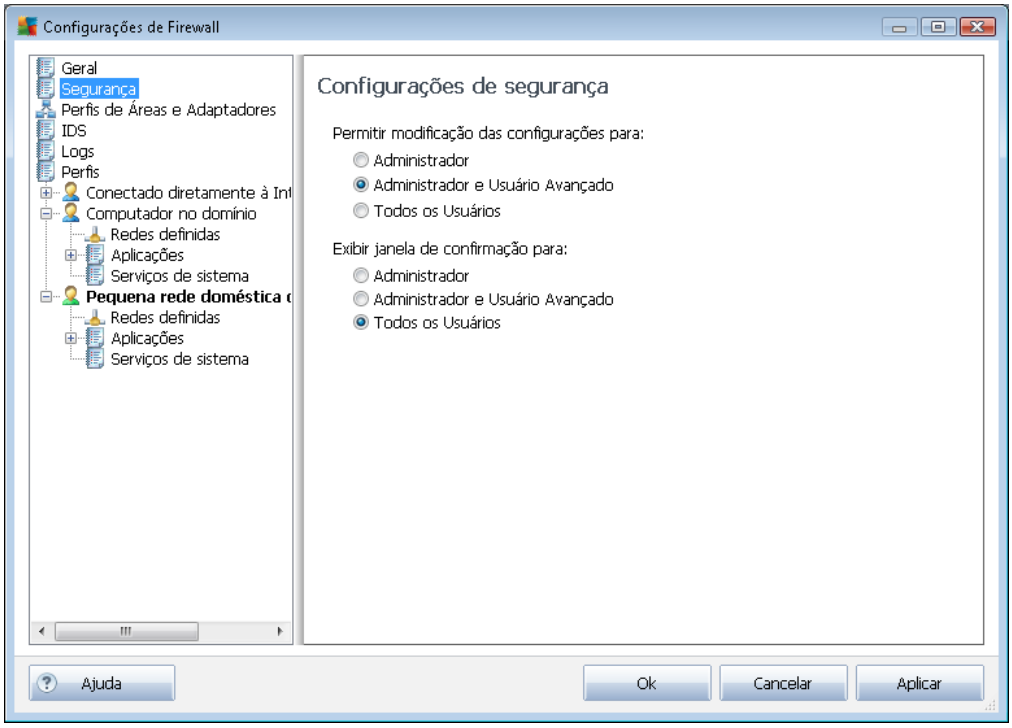
- ***Permitir todo o tráfego para VPN*** *(ativada por padrão)* - se você usa uma conexão VPN *(Rede Privada Virtual)*, como para se conectar de casa com seu escritório, recomendamos que selecione a caixa. ***O AVG Firewall*** irá procurar automaticamente através de adaptadores de rede, encontrar aqueles usados para a conexão VPN, e permitir que todos os aplicativos se conectem à rede de destino *(aplica-se somente a aplicativos com nenhuma regra de firewall específica atribuída)* . Em um sistema padrão com adaptadores de rede comum, essa etapa simples deve evitar que você tenha que configurar uma regra detalhada em cada aplicação que você tenha que usar solução VPN.

Nota: *Para habilitar uma conexão VPN, é necessário permitir comunicação com os seguintes protocolos de sistema: GRE, ESP, L2TP, PPTP. Pode-se fazer isso na caixa de diálogo Serviços do sistema.*

Gerenciamento de configurações

Na seção ***Gerenciamento de configuração***, você pode ***Exportar***/***Importar*** a configuração do Firewall, isto é, exportar as regras e as configurações do Firewall definidas para arquivos de backup ou, por outro lado, importar o arquivo de backup inteiro.

10.2. Segurança



Na caixa de diálogo ***Configurações de segurança***, é possível definir regras gerais de comportamento do Firewall independentemente do perfil selecionado:

- ***Permitir modificação de configurações*** - especifique quem tem permissão para alterar a configuração do Firewall.

- ***Mostrar caixas de diálogo de confirmação*** - especifique para quem as caixas de diálogo de confirmação *(caixas de diálogo que solicitam uma decisão em situações não cobertas por uma regra definida do Firewall)* devem ser exibidas.

Nos dois casos, é possível atribuir o direito específico a um dos seguintes grupos de usuários:

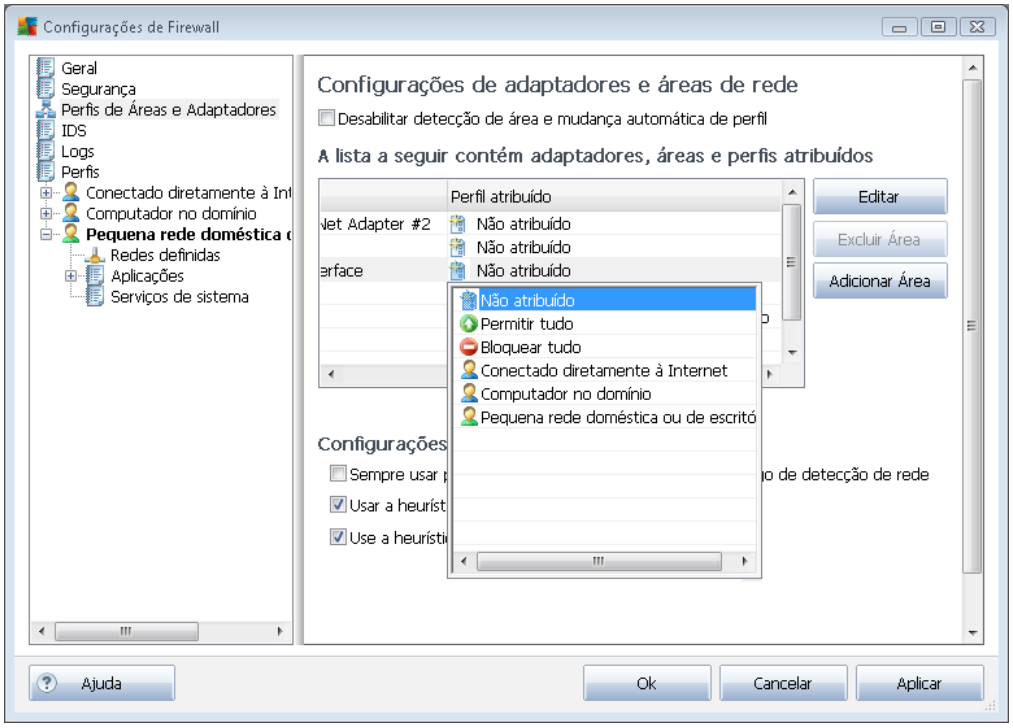
- ***Administrador*** - controla totalmente o computador e tem o direito de atribuir cada usuário a grupos com permissões definidas especificamente.

- ***Administradores e Usuários Avançados*** - o administrador pode atribuir qualquer usuário a um grupo especifico (*Usuários Avançados*) e definir autoridade para os membros do grupo.

- ***Todos os Usuários*** – outros usuários não atribuídos grupos específicos.

10.3. Perfis de áreas e adaptadores

Nas caixas de diálogo ***Configurações de áreas de rede e adaptadores*** , é possível editar as configurações relacionadas à atribuição de perfis definidos a adaptadores específicos e respectivas redes:



- ***Desativar detecção de área e troca automática de perfil*** *(desativada por padrão)* - um dos perfis definidos pode ser atribuído a cada tipo de interface de rede, a cada área

respectivamente. Se você não quiser definir perfis específicos, será usado um perfil comum. Entretanto, se você optar por especificar perfis e atribuí-los a determinados adaptadores e áreas e posteriormente, por algum motivo, quiser trocar esse esquema temporariamente, marque a opção ***Desativar detecção de área e perfil automático***.

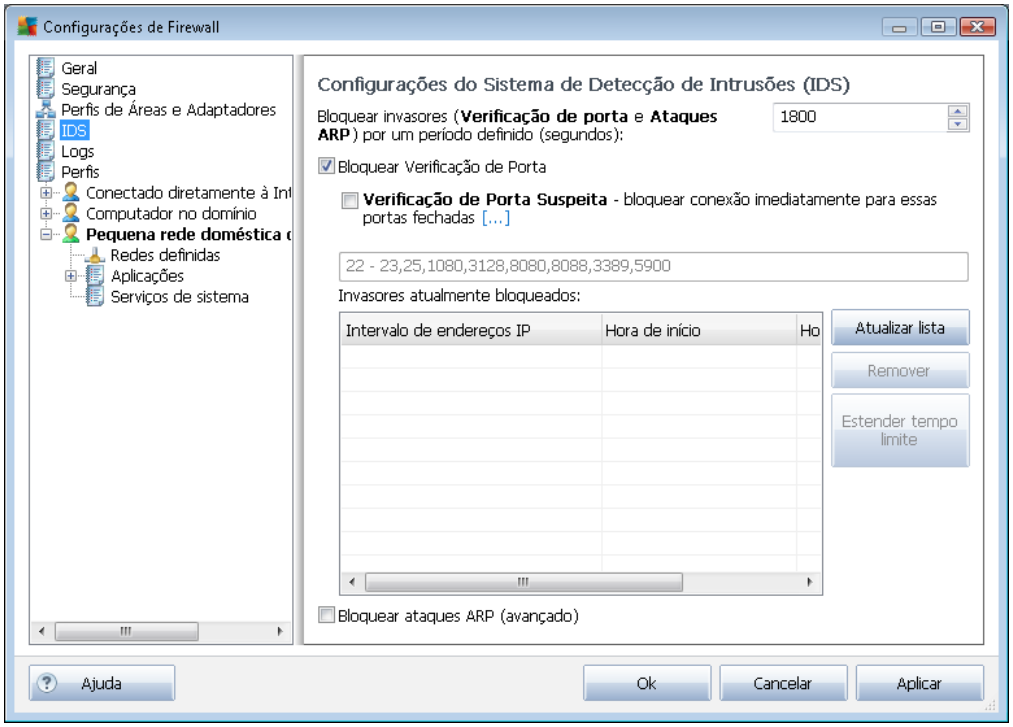
- ***Lista de adaptadores, áreas e perfis atribuídos*** - nesta lista, é possível encontrar uma visão geral de áreas e adaptadores detectados. Para cada um deles, é possível atribuir um perfil específico para o menu de perfis definidos. Para abrir este menu, clique com o botão esquerdo do mouse no item respectivo da lista de adaptadores *(na coluna Perfil atribuído)* e selecione o perfil no menu contextual.

Configurações avançadas

- ***Sempre usar perfil padrão e não exibir nova caixa de diálogo de detecção de rede*** - quando seu computador se conectar a uma nova rede, o Firewall alertará você e exibirá uma caixa de diálogo solicitando que você selecione um tipo de conexão de rede e atribua a ela um perfil de Firewall. Se você não quiser que a caixa de diálogo seja exibida, marque esta caixa.
- ***Usar a heurística AVG para a detecção de novas redes*** - permite obter informações sobre uma rede recém-detectada com o mecanismo próprio do AVG (*no entanto, esta opção está disponível apenas no sistema operacional Windows Vista ou mais recente*).
- ***Usar a heurística Microsoft para a detecção de novas redes*** - permite obter informações sobre uma rede recém-detectada pelo serviço Windows (*esta opção está disponível apenas no Windows Vista ou mais recente*).

10.4. IDS

O Intrusion Detection System (sistema de detecção de intrusão) é um recurso de análise comportamento especial para identificar e bloquear tentativas de comunicação suspeitas em portas específicas de seu computador. Você pode configurar parâmetros do IDS nas configurações da caixa de diálogo ***Sistema de Detecção de Intrusões (IDS)***:



A caixa de diálogo ***Configurações do Sistema de Detecção de Intrusões (IDS)*** oferece estas opções de configuração:

- ***Bloquear invasores (Verificação de porta e Ataques ARP) por um período definido*** - você pode especificar aqui por quantos segundos uma porta ficará bloqueada quando uma tentativa de comunicação suspeita for detectada nela. Por padrão, o intervalo de tempo é definido como 1800 segundos (*30 minutos*).

- ***Bloquear verificação de porta*** *(ativado por padrão)* - marque a caixa para bloquear tentativas de comunicação em todas as portas TCP e UDP com origem externa para o computador. Para tal conexão, cinco tentativas são permitidas, e a sexta é bloqueada. O item está ativado por padrão e recomenda-se que sejam mantidas essas configurações. Se você manter ativada a opção ***Bloquear verificação de porta***, outras configurações mais detalhadas serão disponibilizadas*(caso contrário, o seguinte item será desativado)*:

    - ***Bloquear verificação de porta*** – marque a caixa para bloquear imediatamente qualquer tentativa de comunicação nas portas especificadas no campo de texto abaixo. Portas individuais ou intervalos de portas devem ser divididos por vírgulas. Há uma lista predefinida de portas recomendadas caso você queira usar este recurso.

    - Invasores atualmente bloqueados - esta seção lista qualquer tentativa de comunicação que esteja sendo bloqueada no momento pelo Firewall. Um histórico completo de tentativas bloqueadas pode ser exibido na caixa de diálogo Logs (*guia Logs de verificação de porta*).

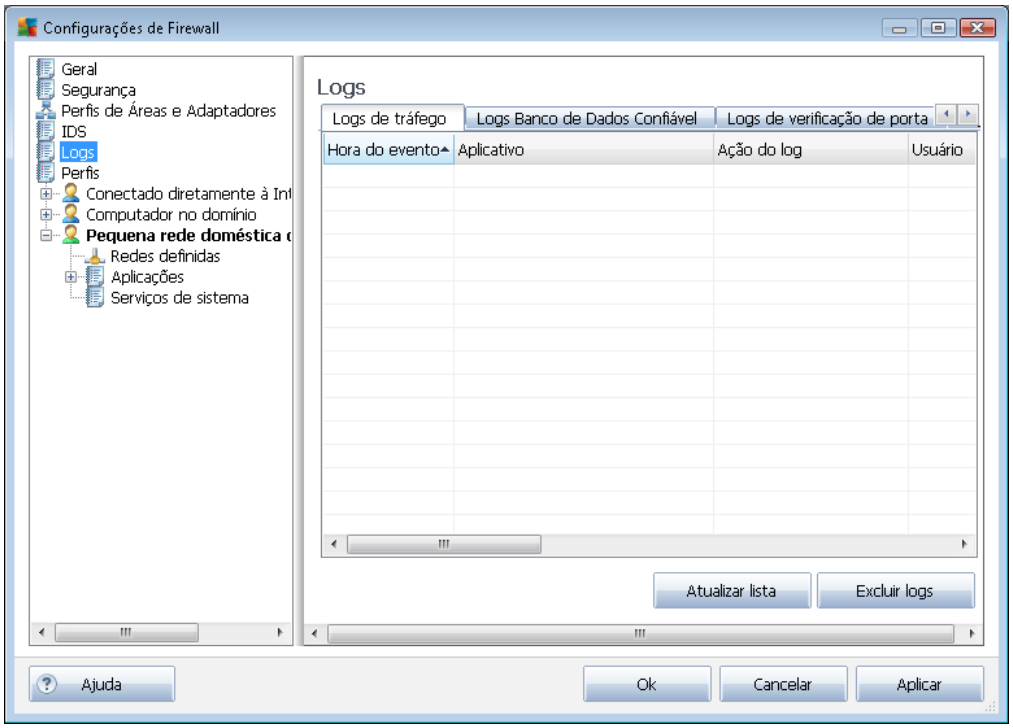
- ***Bloquear ataques ARP (avançado)*** *(ativado por padrão)* - marque esta opção para ativar o bloqueio de tipos especiais de tentativas de comunicação dentro de uma rede local detectada pelo ***IDS*** como possivelmente perigosa. O tempo definido em ***Bloquear***

invasores por um período definido aplica-se. Recomendamos que apenas usuários avançados, familiarizados com o tipo e nível de risco de sua rede local, usem esse recurso.

Botões de controle

- ***Atualizar lista*** - pressione o botão para atualizar a lista (*para incluir todas as tentativas bloqueadas mais recentes*)
- ***Remover*** - pressione para cancelar um bloqueio selecionado
- ***Estender tempo limite*** - pressione para prolongar o período de bloqueio de uma tentativa selecionada. Uma nova caixa de diálogo aparecerá, permitindo que você defina a hora e a data específicas ou uma duração específica.

10.5. Logs



A caixa de diálogo ***Logs*** permite revisar a lista de todas as ações e eventos registrados do Firewall, com uma descrição detalhada dos parâmetros relevantes *(horário do evento, nome do aplicativo, ação respectiva, nome do usuário, PID, direção do tráfego, tipo de protocolo, números das portas remotas e locais, etc.)* em quatro guias:

- ***Logs de tráfego*** - oferece informações sobre atividades de todos os aplicativos que tentaram se conectar à rede.
- ***Logs do banco de dado confiável*** - *O banco de dado confiável* é um banco de dados interno do AVG que coleta informações sobre aplicativos certificados e confiáveis que

sempre têm permissão para se comunicarem on-line. Da primeira vez que um novo aplicativo tentar se conectar à rede (*ou seja, quando ainda não houver uma regra de firewall especificada para esse aplicativo*), será necessário descobrir se a comunicação de rede deve ser permitida para o respectivo aplicativo. Em primeiro lugar, o AVG pesquisa o *Banco de dado confiável* e, se o aplicativo estiver listado, ele receberá acesso automático à rede. Somente depois disso, desde que não haja informações sobre o aplicativo disponíveis no banco de dados, você será solicitado a especificar em uma caixa de diálogo à parte se deseja permitir que esse aplicativo acesse a rede.

- ***Logs de verificação de porta*** - fornece toda de todas as atividades do Sistema de Detecção de Intrusões.

- ***Logs de ARP*** - informações de log ativa sobre o bloqueio de tipos especiais de tentativas de comunicação em uma rede local (opção *Bloquear ataques ARP*) detectados pelo Sistema de Detecção de Intrusões como potencialmente perigosos.

Botões de controle

- ***Atualizar lista*** - todos os parâmetros registrados podem ser organizados de acordo com o atributo selecionado: cronologicamente (*datas*) ou alfabeticamente (*outras colunas*). Basta clicar no respectivo cabeçalho de coluna. Use o botão ***Atualizar lista*** para atualizar as informações exibidas no momento.

- ***Excluir logs*** - pressione esta opção para excluir todas as entradas exibidas.

10.6. Perfis

Na caixa de diálogo ***Configurações do perfil***, é possível encontrar uma lista de todos os perfis disponíveis:

Os Perfis do sistema *(Permitir tudo, Bloquear tudo)* não podem ser editados. No entanto, todos os perfis personalizados*(Conectado diretamente à Internet, Computador no domínio, Pequena rede doméstica ou de escritório)* podem ser editados nesta caixa de diálogo, por meio dos seguintes botões de controle:

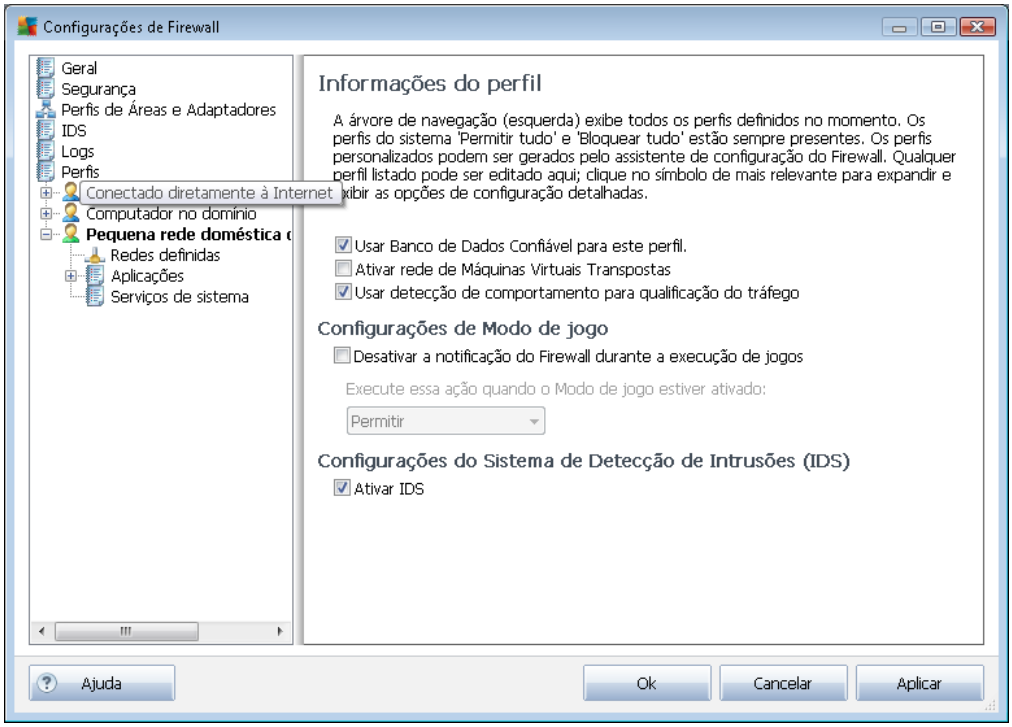
- ***Ativar perfil*** - este botão define o perfil selecionado como ativo, o que significa que a configuração do perfil selecionado será usada pelo Firewall para controlar o tráfego de rede.
- ***Perfil duplicado*** - cria uma cópia idêntica do perfil selecionado. Posteriormente, você poderá editar e renomear a cópia para criar um novo perfil baseado na cópia original duplicada.
- ***Renomear perfil*** - permite definir um novo nome para um perfil selecionado.
- ***Excluir perfil*** - exclui o perfil selecionado da lista.
- ***Alternar banco de dados confiável*** - no perfil selecionado, você pode optar por usar as informações do *Banco de dados confiável* (*o banco de dados confiável é um banco de dados interno do AVG que coleta dados sobre aplicativos confiáveis e certificados que sempre têm permissão de comunicação online.*).
- ***Exportar perfil*** - registra a configuração do perfil selecionado em um arquivo que será salvo para possível uso futuro.

- ***Importar perfil*** - define as configurações do perfil selecionado com base nos dados exportados do arquivo de configuração de backup.

Na seção inferior da caixa de diálogo, localize a descrição de um perfil atualmente selecionado na lista acima.

Com base no número de perfis definidos mencionados na lista da caixa de diálogo ***Perfil***, a estrutura do menu de navegação à esquerda também muda. Cada perfil definido cria uma ramificação específica no item ***Perfil***. Os perfis específicos podem ser editados nas seguintes caixas de diálogo *, que são idênticas para todos os perfis*):

10.6.1. Informações do perfil



A caixa de diálogo ***Informações do perfil*** é a primeira caixa de diálogo de uma seção na qual é possível editar a configuração de cada perfil em caixas de diálogo separadas referentes a parâmetros específicos do perfil.

- ***Usar banco de dados confiável para este perfil*** (*ativado por padrão*) - marque a opção para ativar o *Banco de dados confiável* (*, ou seja, um banco de dados interno do AVG que coleta informações sobre aplicativos confiáveis e certificados que se comunicam online. Se ainda não houver uma regra especificada para o respectivo aplicativo, será necessário descobrir se esse aplicativo pode receber acesso à rede. O AVG pesquisa primeiro o Banco de dados confiável e, se o aplicativo estiver listado, ele será considerado seguro e terá permissão para se comunicar através da rede. Caso contrário, será solicitado que você decida se esse aplicativo deve receber permissão de comunicação na rede*) para o respectivo perfil

- ***Ativar rede de máquinas virtuais em ponte*** (*desativado por padrão*) - marque este item

para permitir que as máquinas virtuais no VMware se conectem diretamente à rede.

- ***Usar detecção comportamental para qualificação do tráfego*** (*ativado por padrão*) - marque esta opção para permitir que o Firewall use a funcionalidade Identity Protection ao avaliar um aplicativo. A Identity Protection pode informar se o aplicativo demonstra um comportamento suspeito ou se é confiável e pode se comunicar online.

Configurações do modo de jogo

Na seção ***Configurações do modo de jogo***, você pode decidir e confirmar, selecionando o respectivo item, se deseja exibir as mensagens de informações do Firewall mesmo durante a execução de um aplicativo de tela cheia no computador (*em geral, são jogos, mas isso se aplica a qualquer aplicativo de tela cheia, como apresentações em PPT*), já que as mensagens de informações podem ser bastante disruptivas.

se você marcar o item ***Desativar notificações do Firewall durante a execução de jogos***, no menu suspenso, e depois selecionar que ação deve ser executada no caso de um aplicativo sem regras especificadas tentar se comunicar pela rede (*aplicativos que normalmente podem gerar uma caixa de diálogo de solicitação*), todos esses aplicativos poderão ser permitidos ou bloqueados.

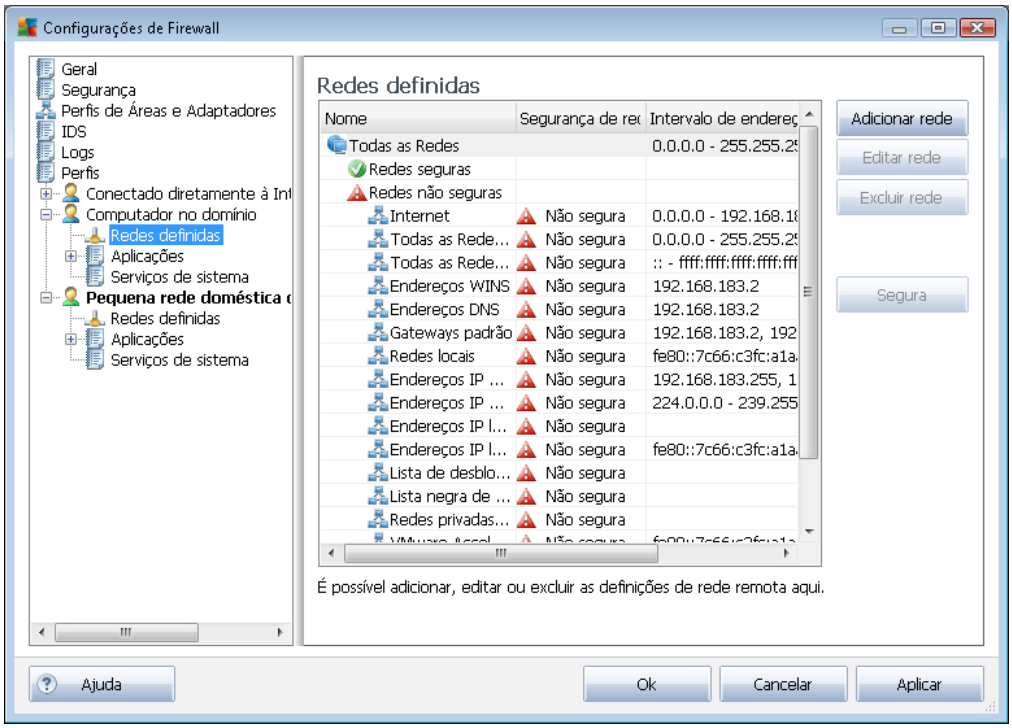
Quando o modo de jogo está ativado, todas as tarefas programadas (*verificações, atualizações*)) são adiadas até que o aplicativo seja fechado.

Configurações do Sistema de Detecção de Intrusões (IDS)

Marque a caixa de seleção ***Ativar IDS*** para ativar o recurso de análise comportamento especial para identificar e bloquear tentativas de comunicação suspeitas em portas específicas de seu computador *(para obter detalhes sobre as configurações desse recurso, consulte o capítulo IDS desta documentação).*

10.6.2. Redes definidas

A caixa de diálogo ***Redes definidas*** oferece uma lista de todas as redes às quais seu computador está conectado.

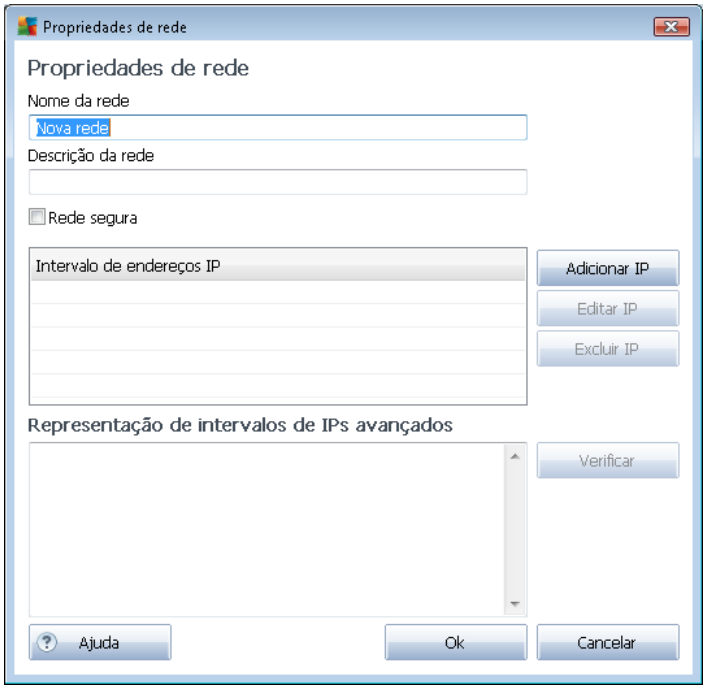


A lista fornece as seguintes informações sobre cada rede detectada:

- ***Redes*** - fornece uma lista de nomes de todas as redes às quais o computador está conectado.
- ***Segurança de rede*** - por padrão, todas as redes são consideradas desprotegidas e somente se tiver certeza de que a respectiva rede é segura você poderá atribuí-la (*clique no item da lista referente à respectiva rede e selecione Seguro no menu de contexto*) - todas as redes seguras serão incluídas no grupo que pode se comunicar com a regra do aplicativo definida para Permitir segurança.
- ***Intervalo de endereços IP*** - cada rede será detectada automaticamente e especificada na forma de intervalo de endereços IP.

Botões de controle

- ***Adicionar rede*** - abre a caixa de diálogo ***Propriedades de rede*** , na qual é possível editar parâmetros da nova rede definida:



Nessa caixa de diálogo, você pode especificar o ***Nome da rede***, fornecer a ***Descrição da rede*** e possivelmente atribuir a rede como segura. A nova rede pode ser definida manualmente em uma caixa de diálogo independente por meio do botão ***Adicionar IP*** (opcionalmente ***Editar IP*** / ***Excluir IP***); nessa caixa de diálogo você pode especificar a rede fornecendo o intervalo IP ou máscara. Em um grande número de redes a serem definidas como parte da nova rede criada, é possível usar a opção ***Representação avançada do intervalo IP***: digite a lista de todas as redes no respectivo campo de texto (*qualquer formato padrão é suportado*) e pressione o botão ***Verificar*** para ter certeza de que o formato pode ser reconhecido. Em seguida, pressione ***OK*** para confirmar e salvar os dados.

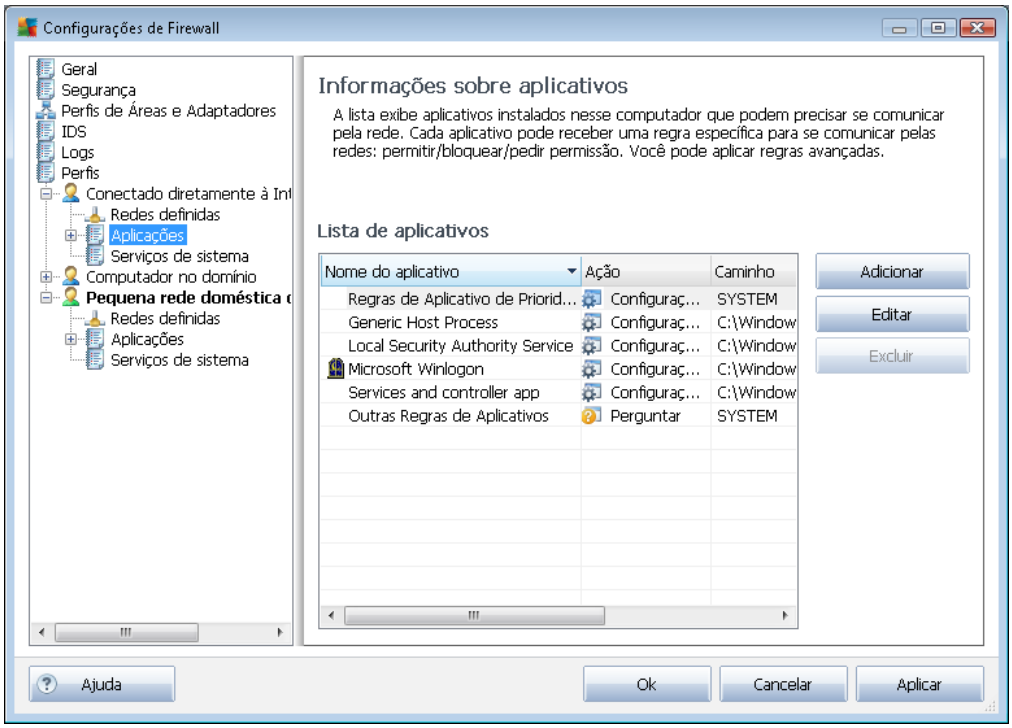
- ***Editar rede*** - abre a caixa de diálogo ***Propriedades da rede*** (*consulte acima*), na qual é possível editar parâmetros de uma rede já definida (*a caixa de diálogo é idêntica à caixa de diálogo de inclusão de nova rede; consulte a descrição no parágrafo anterior*).

- ***Excluir rede*** - remove a nota de uma rede selecionada na lista de redes.

- ***Marcar como seguro*** - por padrão, todas as redes são consideradas desprotegidas, e somente se tiver certeza de que a respectiva rede é segura você poderá usar este botão para atribuí-la (*e vice-versa, uma vez que a rede esteja atribuída como segura, o texto do botão muda para "Marcar como inseguro"*).

10.6.3. Aplicativos

A caixa de diálogo Informações dos aplicativos ***lista todos os aplicativos que possam precisar se comunicar através da rede e ícones para a ação atribuída:***



Os aplicativos na ***Lista de aplicativos*** são aqueles detectados em seu computador (*e que recebem as respectivas ações*). Os seguintes tipos de ação podem ser usados:

- - Permitir comunicação para todas as redes
- - Permitir comunicação somente para redes definidas como Seguras
- - Bloquear comunicação
- - Exibir caixa de diálogo de solicitação (*o usuário poderá decidir se deseja permitir ou bloquear a comunicação quando o aplicativo tentar se comunicar pela rede*)
- - Configurações avançadas definidas

Observe que somente um aplicativo já instalado pode ser detectado. Portanto, se você instalar um novo aplicativo posteriormente, será preciso definir regras de Firewall para ele. Por padrão, quando um novo aplicativo tenta se conectar através da rede pela primeira vez, o Firewall cria uma regra para esse automaticamente, de acordo com o Banco de dados confiável, ou pergunta se deseja permitir ou bloquear a comunicação. Neste último caso, você será capaz de salvar sua resposta como uma regra permanente (que será listada nesta caixa de diálogo).

É claro, você pode definir regras para o novo aplicativo imediatamente – nessa caixa de diálogo,

pressione ***Adicionar*** e preencha os detalhes do aplicativo.

Além dos aplicativos, a lista também contém dois itens especiais:

- ***Regras prioritárias do aplicativo*** *(na parte superior da lista) são preferenciais e são aplicadas sempre antes das regras de qualquer aplicativo individual.*
- ***Outras regras de aplicativos*** *(na parte inferior da lista) são usadas como uma "última instância", quando não é aplicada nenhuma regra específica; por exemplo, para um aplicativo desconhecido e não definido.*

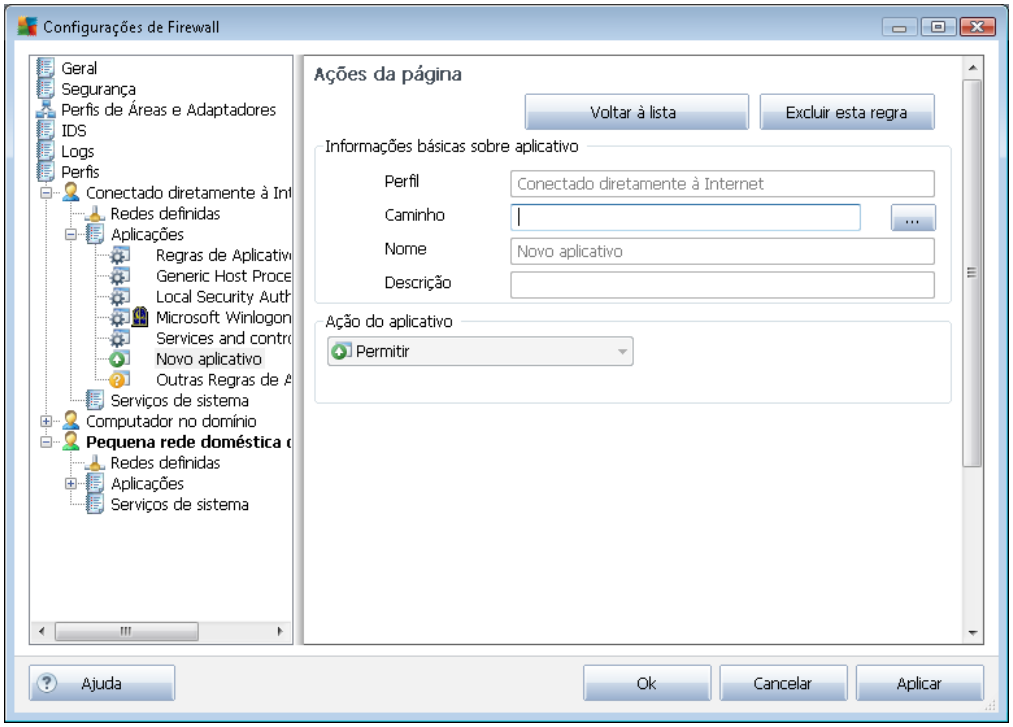
Esses itens têm diferentes opções de configuração em relação aos aplicativos comuns e são destinados somente a usuários experientes. Recomendamos fortemente que você não modifique as configurações!

Botões de controle

É possível editar a lista usando os seguintes botões de controle:

- ***Adicionar*** - abre uma caixa de diálogo vazia Ações da página para definir novas regras de aplicativo.
- ***Editar*** - abre a mesma caixa de diálogo Ações da página para edição de um conjunto de regras de um aplicativo existente.
- ***Excluir*** - remove o aplicativo selecionado da lista.

Na caixa de diálogo ***Ações da página***, você pode definir as configurações do respectivo aplicativo em detalhes:



Botões de controle

Dois botões de controle estão disponíveis na parte superior da caixa de diálogo:

- ***Voltar à lista*** - pressione o botão para exibir a visão geral de todas as regras dos aplicativos definidos.
- ***Excluir esta regra*** - clique neste botão para apagar a regra de aplicativo exibida no momento. ***Observe que esta ação não pode ser revertida!***

Informações básicas sobre aplicativo

Nesta seção, preencha o ***Nome*** do aplicativo e, opcionalmente, uma ***Descrição*** *(um breve comentário para sua informação)*. No campo ***Caminho***, insira todo o caminho para o aplicativo (o arquivo executável) no disco; como alternativa, você pode localizar o aplicativo na estrutura em árvore de maneira conveniente após pressionar o botão "...".

Ação do aplicativo

No menu suspenso, você pode selecionar a regra do Firewall para o aplicativo, ou seja, o que o

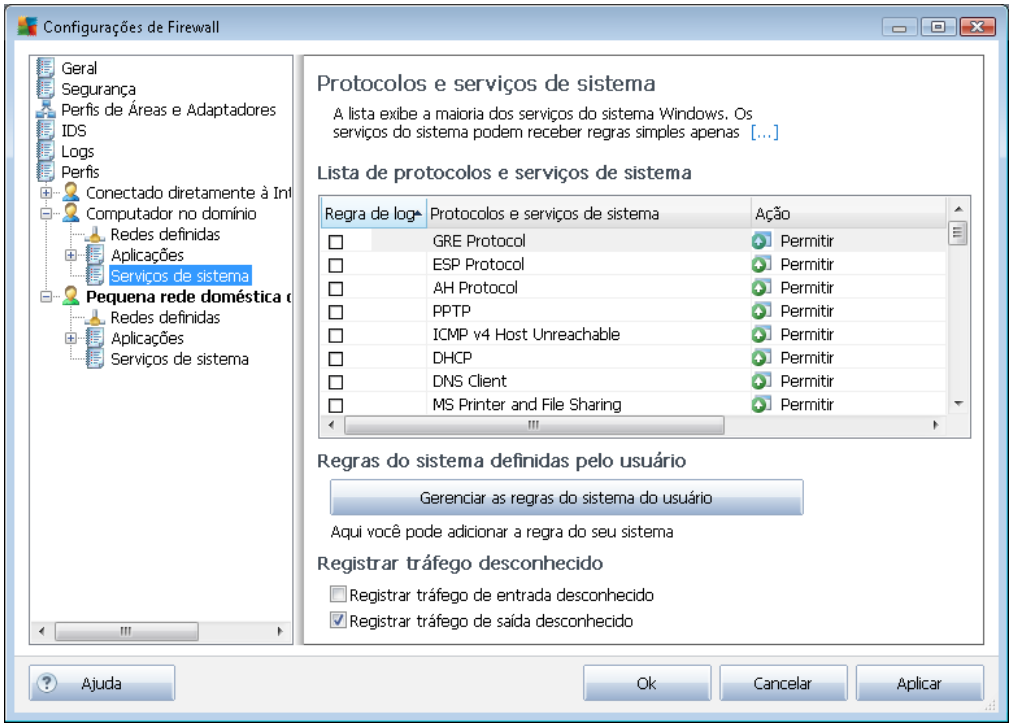
Firewall deve fazer quando o aplicativo tentar se comunicar através da rede:

- ***Permitir para todos*** - permite que o aplicativo se comunique em todas as redes e os adaptadores definidos sem limitações.
- ***Permitir redes seguras*** permitirá que o aplicativo se comunique em todas as redes definidas como seguras *(confiáveis)*.
- ***Bloquear*** - impede a comunicação automaticamente. O aplicativo não terá permissão para se conectar a nenhuma rede.
- ***Solicitar*** - exibe uma caixa de diálogo permitindo que você opte por permitir ou bloquear a tentativa de comunicação naquele momento.
- ***Configurações avançadas*** - exibe opções de configuração ainda mais avançadas e detalhadas na parte inferior da caixa de diálogo na seção ***Regras de detalhes do aplicativo***. Os detalhes serão aplicados de acordo com a ordem da lista, de modo que você poderá ***Promover*** ou ***Rebaixar*** as regras da lista conforme o necessário para estabelecer sua precedência. Após clicar em uma regra específica na lista, a visão geral dos detalhes da regra será exibida na parte inferior da caixa de diálogo. Qualquer valor em azul sem link pode ser alterado na caixa de diálogo clicando na respectiva configuração. Para excluir a regra destacada, simplesmente pressione***Remover***. Para definir uma nova regra, use o botão ***Incluir***para abrir a caixa de diálogo***Alterar detalhe de regra*** que lhe permite especificar todos os detalhes necessários.

10.6.4. Serviços do sistema

As edições na caixa de diálogo Protocolos e serviços do sistema SÓ DEVEM SER FEITAS POR USUÁRIOS EXPERIENTES.

A caixa de diálogoProtocolos e serviços do sistema ***lista os protocolos e os serviços do sistema padrão do Windows que possam precisar se comunicar através da rede:***



Lista de protocolos e serviços de sistema

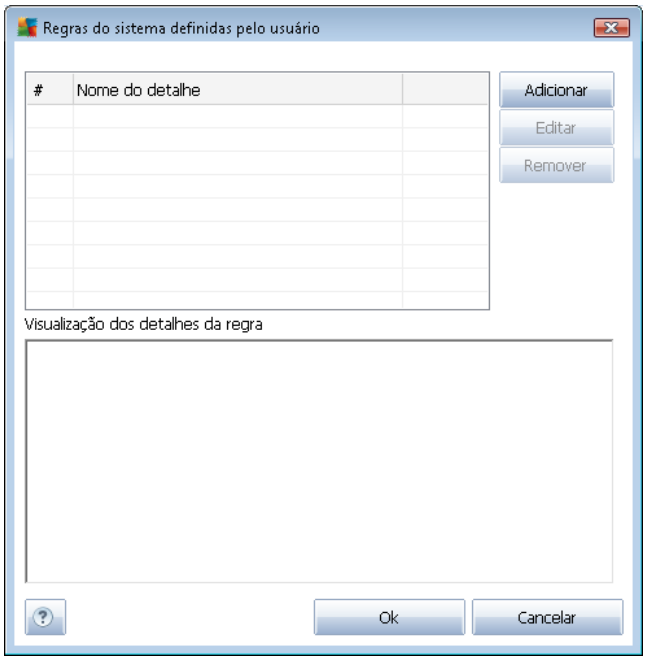
O gráfico contém as seguintes colunas:

- ***Ação de regra de log*** - esta caixa permite que você ative o registro de cada aplicativo de regra nos logs.
- ***Protocolos e serviços do sistema*** - esta coluna mostra um nome do respectivo serviço do sistema.
- ***Ação*** - esta coluna exibe um ícone para a ação atribuída:
  - Permitir comunicação para todas as redes
  - Permitir comunicação somente para redes definidas como Seguras
  - Bloquear comunicação
- ***Redes*** - esta coluna declara a qual rede específica a regra do sistema se aplica.

Para editar as configurações de qualquer item na lista (incluindo as ações atribuídas), dê um clique com o botão direito no item e selecione ***Editar***. ***Entretanto, uma edição das regras do sistema deve ser feita apenas por usuários avançados, e é altamente recomendado não editar as regras de sistema!***

Regras do sistema definidas pelo usuário

Para abrir uma nova caixa de diálogo para definir sua própria regra de serviço do sistema, veja a figura abaixo e pressione o botão ***Gerenciar as regras do sistema do usuário.*** ***A seção superior da caixa de diálogo Regras do sistema definidas pelo usuário***exibe a visão geral de todos os detalhes da regra do sistema editada no momento; a seção inferior exibe o detalhe selecionado. Detalhes da regra definida pelo usuário podem ser editados, adicionados ou excluídos pelo botão respectivo; detalhes da regra definida pelo fabricante só podem ser editados:



Observe que estas configurações dos detalhes da regra são avançadas, destinadas principalmente para administradores de rede que necessitam de controle total sobre a configuração de Firewall. Se você não estiver familiarizado com os tipos de protocolos de comunicação, números de porta de rede, definições de endereço IP etc, não modifique estas definições! Se você realmente precisa alterar a configuração, consulte os arquivos de ajuda da caixa de diálogo respectiva para detalhes específicos.

Registrar tráfego desconhecido

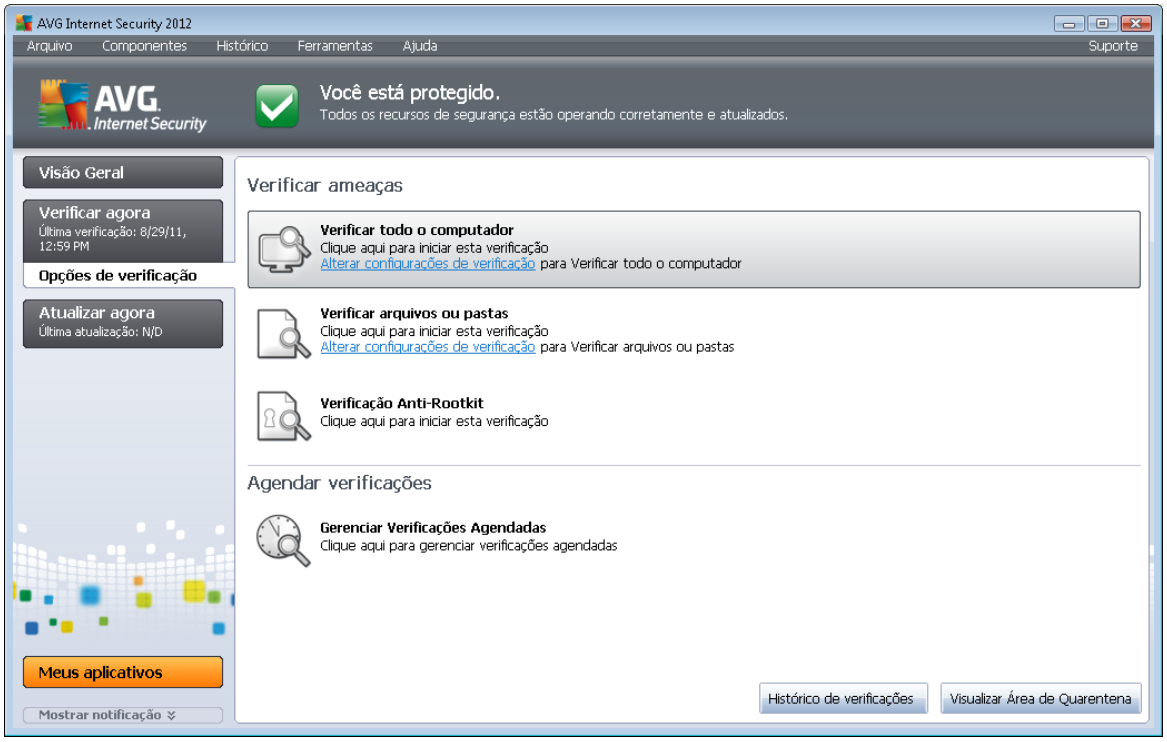
- ***Registrar tráfego de entrada desconhecido*** *(desativado por padrão)* - marque a caixa para registrar nos Logs toda tentativa externa desconhecida de conexão com o seu computador.

- ***Registrar em log o tráfego de saída desconhecido*** *(ativado por padrão)* - marque a caixa para registrar nos Logs qualquer tentativa desconhecida do seu computador para se conectar a um local externo.

11. Verificação do AVG

Por padrão, o **AVG Internet Security 2012** não executa verificações, já que, após a verificação inicial, você deverá estar totalmente protegido pelos componentes residentes do **AVG Internet Security 2012**, que estão sempre em guarda e não permitem que códigos mal-intencionados entrem em seu computador. No entanto, você pode agendar uma verificação para que seja executada em intervalos regulares ou iniciar uma verificação manual, de acordo com suas necessidades, a qualquer momento.

11.1. Interface da verificação



A interface de verificação do AVG pode ser acessada pelo link rápido ***Opções de verificação***. Clique nesse link para passar para a caixa de diálogo ***Verificar ameaças*** . Nessa caixa de diálogo, você encontrará o seguinte:

- visão geral das verificações predefinidas - três tipos de verificação definidos pelo fornecedor do software estão prontos para uso imediato sob demanda ou de forma programada:
  - Verificação de todo o computador
  - Verificar arquivos ou pastas específicas
  - Verificação Anti-Rootkit
- seção programação da verificação - onde é possível definir novos testes e criar novas programações, conforme necessário.

Botões de controle

Os botões de controle disponíveis na interface de teste são:

- ***Histórico da verificação*** - exibe a caixa de diálogo Visão geral dos resultados da verificação com todo o histórico da verificação
- ***Exibir Quarentena*** - abre uma nova janela com a Quarentena - um espaço em que as infecções detectadas são colocadas em quarentena

11.2. Verificações predefinidas

Um dos principais recursos do **AVG Internet Security 2012** é a verificação sob demanda. Testes sob demanda são desenvolvidos para verificar várias partes do seu computador, sempre que surgir a suspeita de uma possível infecção por vírus. De qualquer forma, é altamente recomendável realizar esses testes regularmente, ainda que você ache que nenhum vírus possa ser encontrado em seu computador.

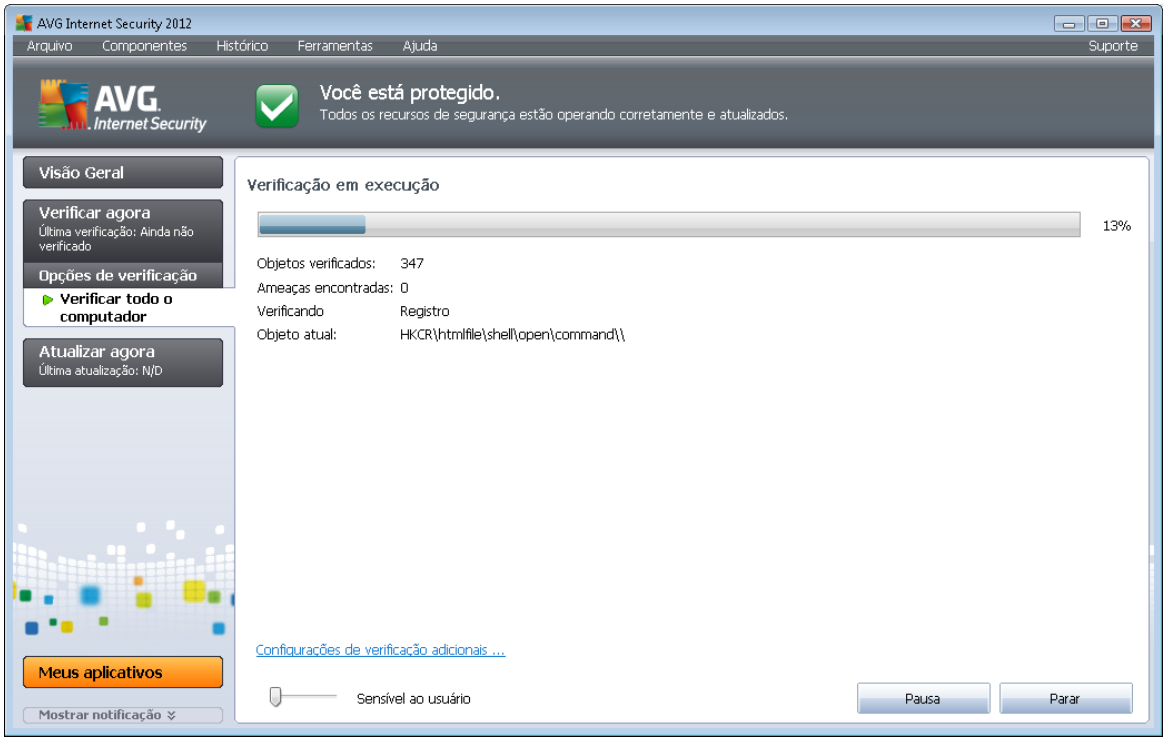
No **AVG Internet Security 2012** você encontrará os seguintes tipos de verificação predefinidos pelo fornecedor do software:

11.2.1. Verificação de todo o computador

Verificar todo o computador - verifica todo o computador em busca de infecções e/ou programas potencialmente indesejáveis. Esse teste verificará todos os discos rígidos do computador, detectará e reparará qualquer vírus encontrado ou removerá a infecção para a Quarentena de vírus. A verificação de todo o computador deve ser programada em uma estação de trabalho pelo menos uma vez por semana.

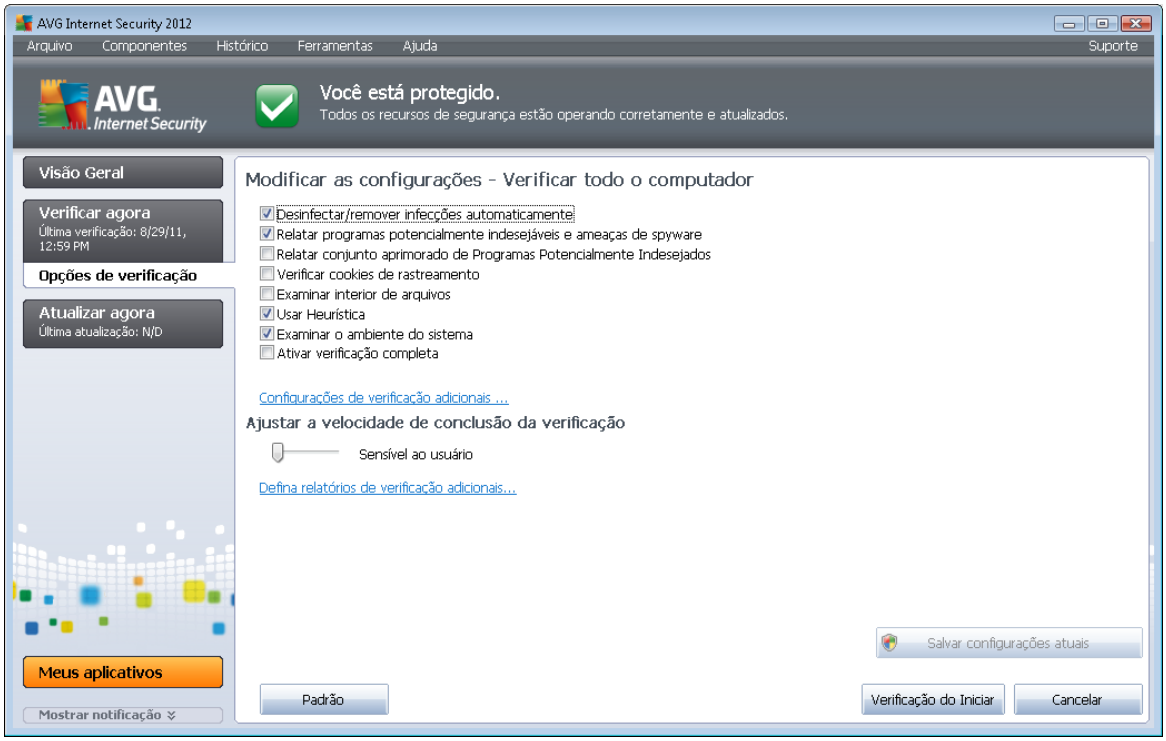
Iniciar verificação

Verificar todo o computador pode ser iniciado diretamente na interface de verificação, clicando no ícone de verificação. Se nenhuma outra configuração específica for configurada para esse tipo de verificação, ela será iniciada imediatamente dentro da caixa de diálogo de ***Verificação em andamento*** *(veja a imagem)*. A verificação pode ser interrompida temporariamente (***Pausar***) ou cancelada (***Parar***) se necessário.



Verificar edições de configuração

Você tem a opção de editar as configurações padrão predefinidas de ***Verificar todo o computador***. Clique no link ***Alterar as configurações de verificação*** para acessar a caixa de diálogo ***Alterar configurações de verificação de Verificar todo o computador*** *(acessível pela interface de verificação por meio do link Alterar as configurações de verificação para Verificar todo o computador)*. ***É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.***



- ***Parâmetros de verificação*** - na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades:

    - ***Reparar ou remover infecção automaticamente*** (*ativada por padrão*) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

    - ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo Anti-Spyware e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

    - ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

    - ***Verificar cookies de rastreamento*** (*desativada por padrão*) - este parâmetro do componente Anti-Spyware define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras*

eletrônicas).

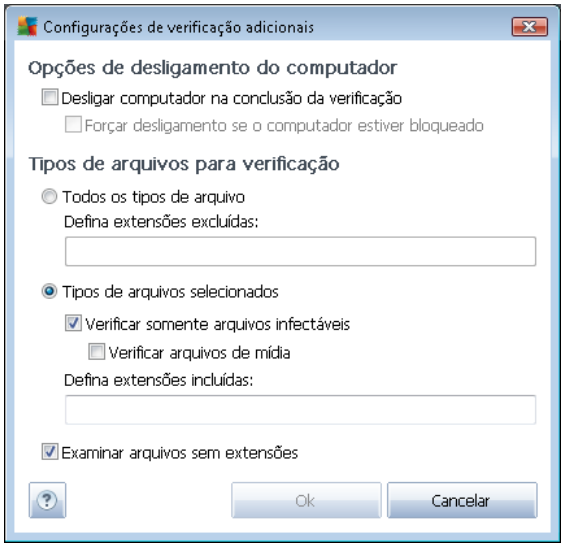
- ***Verificar dentro dos arquivos*** (*desativada por padrão*) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

- ***Usar Heurística*** (*ativada por padrão*) - a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação

- ***Verificar ambiente do sistema*** (*ativada por padrão*) - a verificação também atuará nas áreas do sistema do seu computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, na qual é possível especificar os seguintes parâmetros:



- ***Opções de desligamento do computador*** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Tipos de arquivo para verificação*** - além disso, você deve decidir se deseja verificar os seguintes itens:

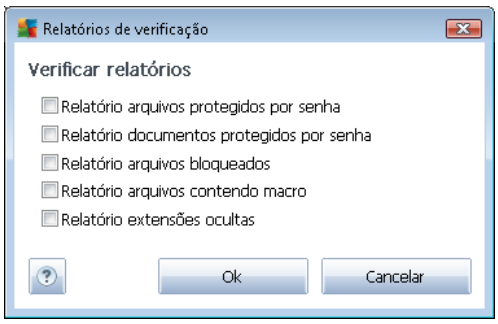
- ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

- ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

- Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Ajustar a velocidade de conclusão da verificação*** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de descobertas devem ser relatados:



Aviso: *essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo Verificação do AVG/Programação da verificação/ Como verificar. Se você decidir alterar as configurações padrão de* ***Verificar todo o computador****, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de todo o computador.*

11.2.2. Verificar arquivos ou pastas específicos

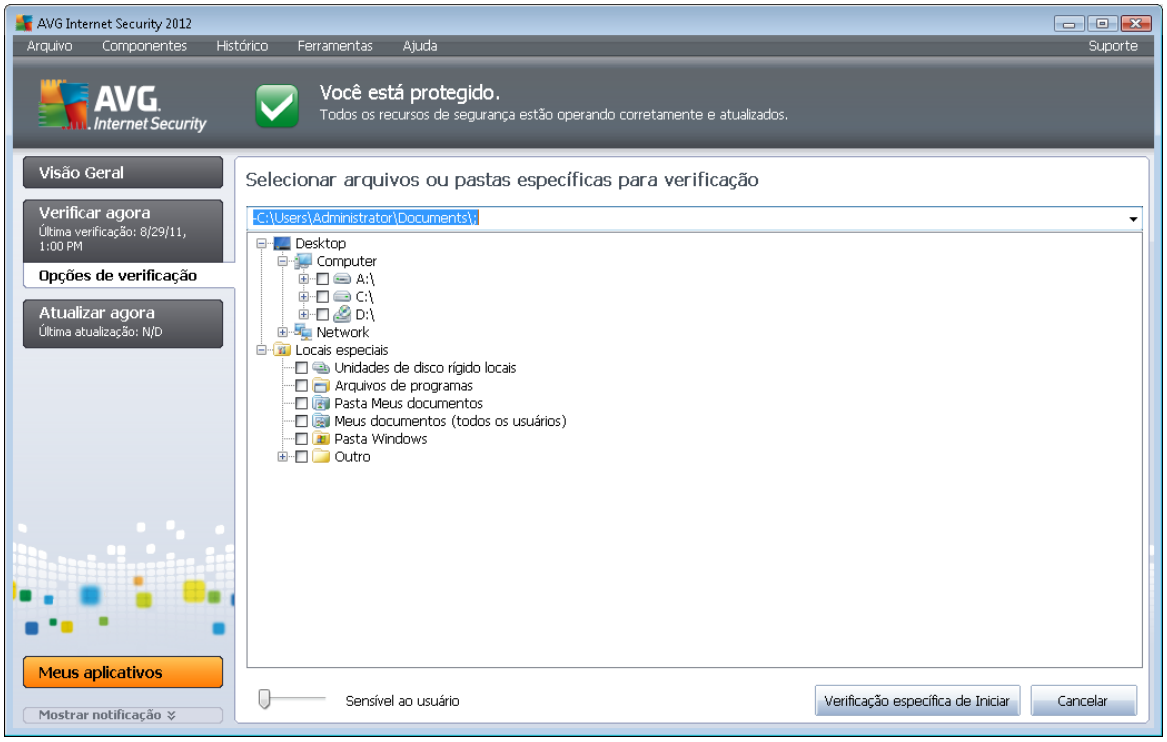
Verificar arquivos ou pastas específicos - verifica somente as áreas do computador que você tenha selecionado para verificação (*pastas selecionadas, discos rígidos, unidades de disquete, CDs etc.*). O andamento da verificação em caso de detecção e tratamento de vírus é o mesmo da verificação de todo o computador: todos os vírus encontrados serão reparados ou removidos para a Quarentena de vírus. A verificação de arquivos ou pastas específicos pode ser usada para configurar seus próprios testes e sua programação com base nas necessidades.

Iniciar verificação

A opção ***Verificar arquivos ou pastas específicos*** pode ser iniciada diretamente na interface de verificação clicando no ícone de verificação. Uma nova caixa de diálogo chamada ***Selecionar arquivos ou pastas específicos para verificação*** será aberta. Na estrutura de árvores do computador, selecione as pastas que deseja verificar. O caminho para cada pasta selecionada será gerado automaticamente e exibido na caixa de texto na parte superior dessa caixa de diálogo.

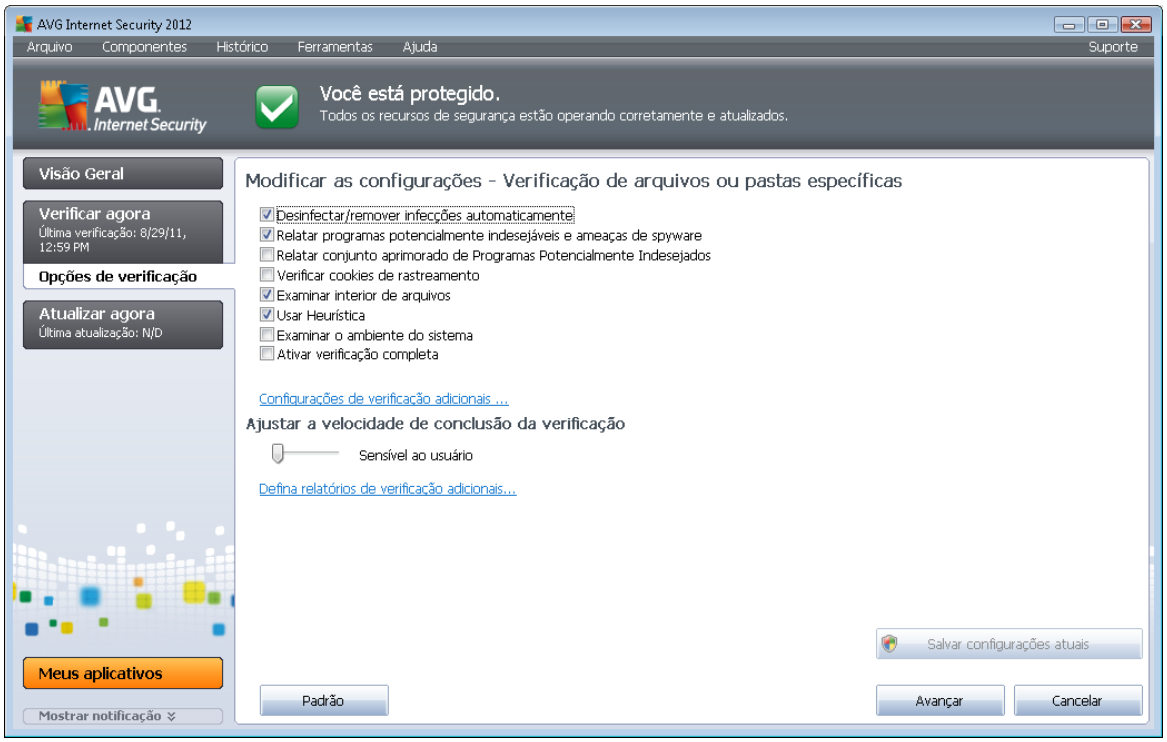
Também existe a possibilidade de fazer a verificação em uma determinada pasta enquanto suas subpastas são excluídas da verificação; para isso, insira um sinal de menos "**-**" na frente do caminho gerado automaticamente (*veja a imagem*). Para excluir da verificação a pasta inteira, use o parâmetro "**!**" .

Finalmente, para iniciar a verificação, pressione o botão ***Iniciar verificação***; o processo de verificação será basicamente idêntico a Verificar todo o computador.



Verificar edições de configuração

Você tem a opção de editar as configurações padrão predefinidas de ***Verificar arquivos ou pastas específicos***. Acesse o link ***Alterar as configurações de verificação*** para abrir a caixa de diálogo ***Alterar configurações de verificação de Verificar arquivos ou pastas específicos***. ***É recomendável manter as configurações padrão, a menos que você tenha um motivo válido para alterá-las.***



- ***Parâmetros de verificação*** - na lista de parâmetros de verificação, você pode ativar ou desativar parâmetros específicos conforme suas necessidades:

    - ***Reparar ou remover infecção automaticamente*** (*ativada por padrão*) - se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Se o arquivo infectado não puder ser reparado automaticamente, o objeto infectado será movido para a Quarentena de Vírus.

    - ***Informar programas potencialmente indesejáveis e ameaças de spyware*** (*ativada por padrão*) - marque para ativar o mecanismo Anti-Spyware e verificar se há spyware e vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

    - ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*) - marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do

fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*) - este parâmetro do componente Anti-Spyware define que os cookies devem ser detectados; (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*).

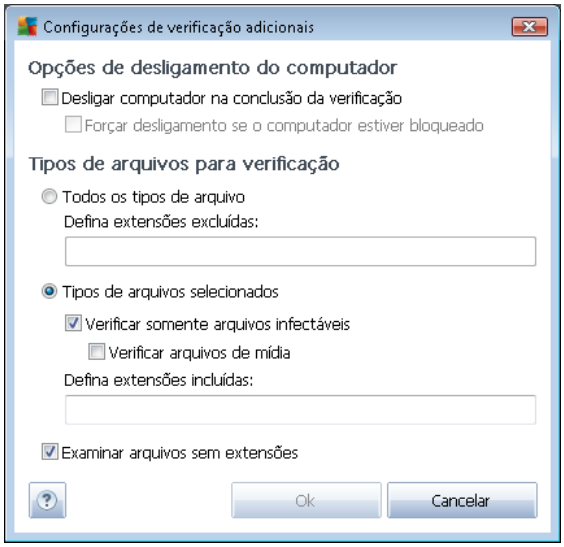
- ***Verificar dentro dos arquivos*** (*ativada por padrão*) - esse parâmetro define que a verificação deve ocorrer em todos os arquivos armazenados dentro de arquivos, como ZIP, RAR etc.

- ***Usar heurística*** (*desativada por padrão*) - a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação.

- ***Verificar ambiente do sistema*** (*desativada por padrão*) - a verificação também atuará nas áreas do sistema do seu computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, na qual é possível especificar os seguintes parâmetros:



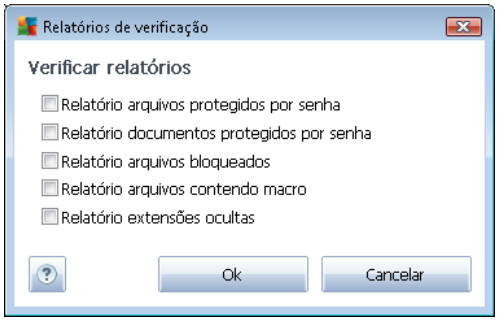
- ***Opções de desligamento do computador*** - decida se o computador deve ser

desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Tipos de arquivo para verificação*** - você também deve decidir se deseja verificar os seguintes itens:
  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.
  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Prioridade do processo de verificação*** - você pode usar esse controle para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais tipos de possíveis localizações devem ser relatados:



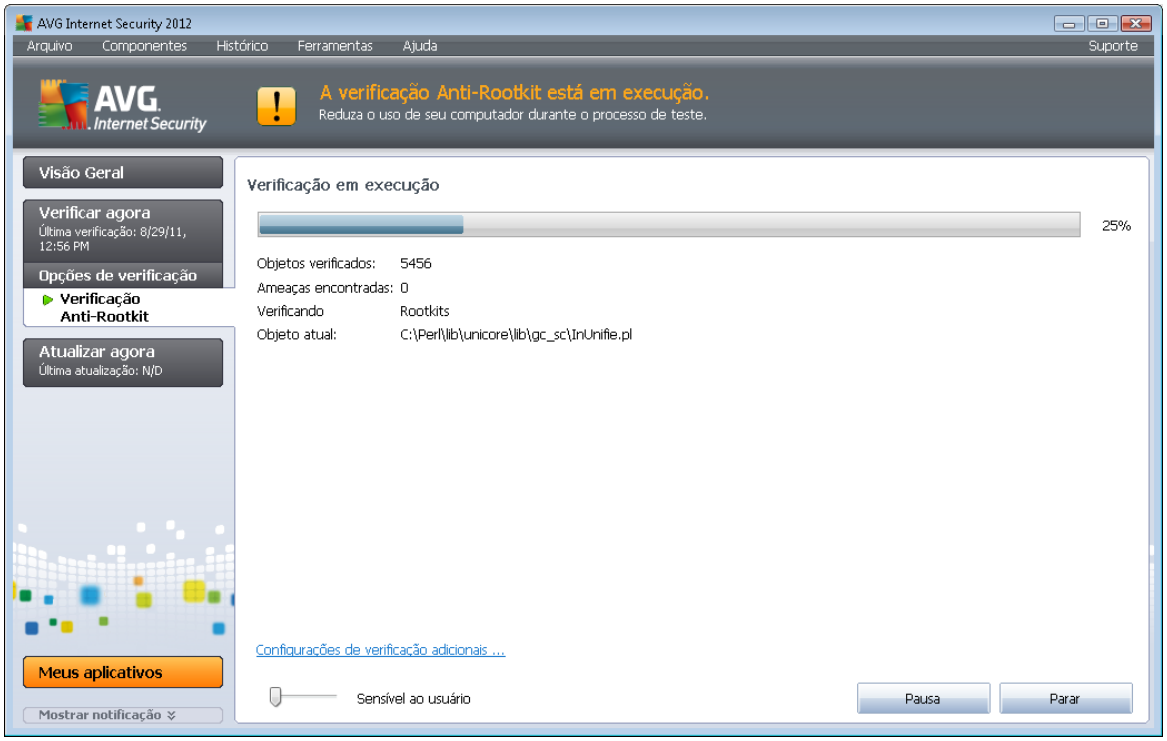
Aviso: *essas configurações de verificação são idênticas aos parâmetros de uma verificação definida recentemente, como descrito no capítulo Verificação do AVG/Programação da verificação/ Como verificar. Se você decidir alterar as configurações padrão de* ***Verificar arquivos ou pastas específicas****, será possível salvar as novas configurações como o padrão a ser usado para todas as verificações futuras de arquivos ou pastas específicas. Além disso, essa configuração será usada como modelo para todas as novas verificações programadas (todas as verificações personalizadas são baseadas na configuração atual de Verificação de arquivos ou pastas selecionados).*

11.2.3. Verificação Anti-Rootkit

A Verificação Anti-Rootkit verifica seu computador em busca de possíveis rootkits (*programas e tecnologias que possam ocultar atividades de malware no computador*). Se um rootkit for detectado, isso não quer dizer necessariamente que o computador está infectado. Em alguns casos, drivers específicos ou seções de aplicativos comuns podem ser detectados por engano como rootkits.

Iniciar verificação

A Verificação Anti-Rootkit pode ser iniciada diretamente na interface de verificação clicando no ícone de verificação. Se nenhuma outra configuração específica for definida para esse tipo de verificação, ela será iniciada imediatamente na caixa de diálogo ***Verificação em andamento*** *(veja a imagem)*. A verificação pode ser interrompida temporariamente (***Pausar***) ou cancelada (***Parar***), se necessário.

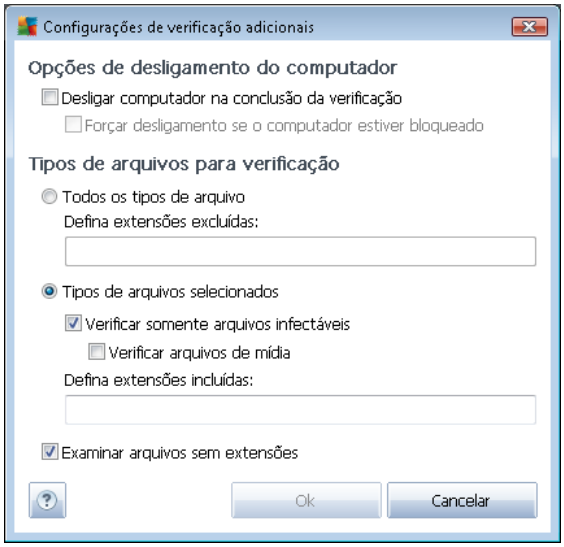


Verificar edições de configuração

A Verificação Anti-Rootkit é sempre iniciada nas configurações padrão, e a edição dos parâmetros de verificação só pode ser acessada na caixa de diálogo Configurações avançadas do AVG/Anti-Rootkit. Na interface de verificação, a seguinte configuração está disponível, mas apenas enquanto a verificação está em execução:

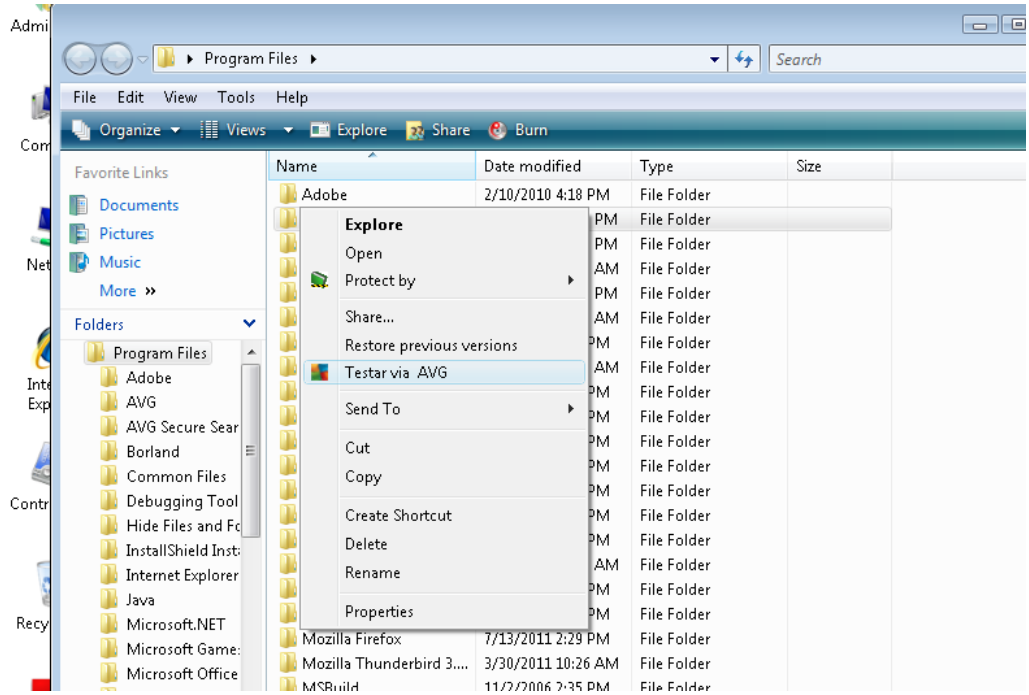
- ***Verificação automática*** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Configurações de verificação adicionais*** - este link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, na qual você pode definir possíveis condições de desligamento do computador relacionadas à ***Verificação Anti-Rootkit*** (***Desligar o computador após a conclusão da verificação*** e *possivelmente* ***Forçar encerramento se o computador estiver travado***):



11.3. Verificando o Windows Explorer

Além das verificações predefinidas iniciadas em todo o computador ou em áreas selecionadas, o **AVG Internet Security 2012 ainda oferece a opção de uma verificação rápida de um objeto específico diretamente no ambiente do Windows Explorer.** Se você desejar abrir um arquivo desconhecido e não tiver certeza sobre o seu conteúdo, poderá verificá-lo sob demanda. Siga estas etapas:



- No Windows Explorer, realce o arquivo *(ou a pasta)* que deseja verificar
- Clique com o botão direito do mouse no objeto para abrir o menu de contexto
- Selecione a opção ***Verificar com*** para que o arquivo seja verificado com o AVG**AVG Internet Security 2012**

11.4. Verificação de linha de comando

No **AVG Internet Security 2012** há a opção de executar a verificação a partir da linha de comando. Você pode usar esta opção em servidores, ou ao criar um script em lote para ser iniciado automaticamente após a inicialização do computador. A partir da linha de comando, você pode iniciar a verificação com a maioria dos parâmetros como oferecido em uma interface gráfica de usuário AVG.

Para iniciar a verificação AVG da linha de comando, execute o seguinte comando dentro da pasta em que o AVG está instalado:

- ***avgscanx*** para SO de 32 bits
- ***avgscana*** para SO de 64 bits

Sintaxe do comando

A seguir, a sintaxe do comando:

- ***avgscanx /parâmetro*** ... por exemplo. ***avgscanx /comp*** para verificação de todo o

computador

- ***avgscanx /parâmetro /parâmetro*** .. com vários parâmetros, estes devem estar alinhados em uma fila e separados por um espaço e um caractere de barra

- se o parâmetro exigir um valor específico a ser fornecido (por exemplo, o parâmetro ***/scan*** requer informações sobre quais são as áreas selecionadas do seu computador a serem verificadas, e você precisa informar o caminho exato da seção selecionada), os valores serão divididos por ponto e vírgula, como por exemplo: ***avgscanx /scan=C:\;D:***

Parâmetros de verificação

Para exibir uma visão completa dos parâmetros disponíveis, digite o respectivo comando junto com o parâmetro /? ou /HELP (por ex., ***avgscanx /?***). O único parâmetro obrigatório é /SCAN, que especifica que áreas do computador que devem ser verificadas. Para obter uma explicação mais detalhada das opções, consulte a visão geral dos parâmetros da linha de comando.

Para executar a verificação, pressione ***Enter***. Durante a verificação, você pode interromper o processo ao pressionar ***Ctrl+C*** ou ***Ctrl+Pause***.

Verificação CMD iniciada pela interface gráfica

Quando você executa seu computador no Modo de segurança do Windows, também é possível iniciar a verificação das linhas de comando pela interface gráfica do usuário. A verificação será iniciada pela linha de comando; a caixa de diálogo ***Composer da linha de comando*** apenas permite que você especifique a maioria dos parâmetros de verificação na interface gráfica amigável.

Como esta caixa de diálogo está acessível apenas pelo Modo de segurança do Windows, para obter uma descrição detalhada dela consulte o arquivo de ajuda acessível diretamente pela caixa de diálogo.

11.4.1. Parâmetros de verificação CMD

A seguir, veja uma lista de todos os parâmetros disponíveis para a verificação de linha de comando:

- ***/SCAN*** Verificar arquivos ou pastas específicos */SCAN=path;path (e.x. /SCAN=C:\;D:\)*
- ***/COMP*** Verificar todo o computador
- ***/HEUR*** Usar análise heurística
- ***/EXCLUDE*** Excluir caminho ou arquivo da verificação
- ***/@*** Arquivo de comando/nome de arquivo/
- ***/EXT*** Verificar estas extensões/por exemplo, EXT=EXE,DLL
- ***/NOEXT*** Não verificar estas extensões/por exemplo, NOEXT=JPG/

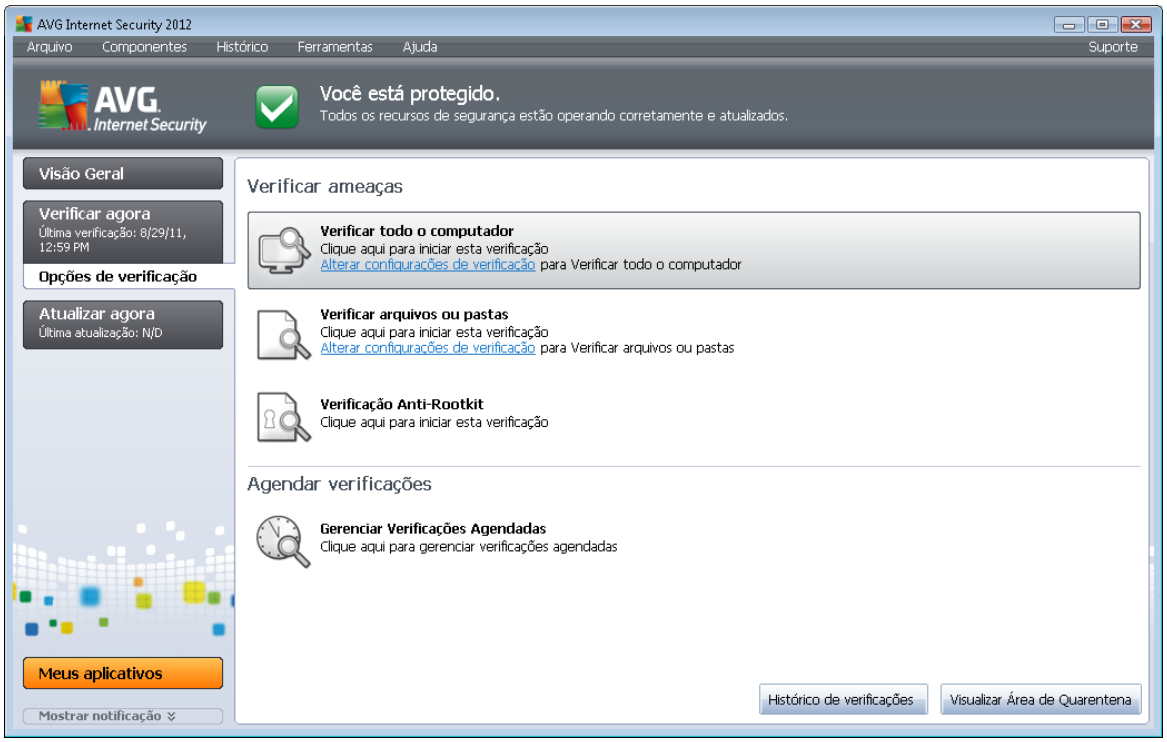
- ***/ARC*** Verificar arquivos
- ***/CLEAN*** Limpar automaticamente
- ***/TRASH*** Mover arquivos infectados para a Quarentena de vírus
- ***/QT*** Teste rápido
- ***/MACROW*** Relatar macros
- ***/PWDW*** Relatar arquivos protegidos por senha
- ***/IGNLOCKED*** Ignorar arquivos bloqueados
- ***/REPORT*** Relatar para arquivo/ nome de arquivo/
- ***/REPAPPEND*** Acrescentar ao arquivo de relatório
- ***/REPOK*** Relatar arquivos não infectados como OK
- ***/NOBREAK*** Não permitir abortar com CTRL-BREAK
- ***/BOOT*** Ativar verificação de MBR/BOOT
- ***/PROC*** Verificar processos ativos
- ***/PUP*** Relatar "Programas potencialmente indesejáveis"
- ***/REG*** Verificar registro
- ***/COO*** Verificar cookies
- ***/?*** Exibir ajuda neste tópico
- ***/HELP*** Exibir ajuda neste tópico
- ***/PRIORIDADE*** Defina a prioridade da verificação /Baixa, Automática, Alta/ *(consulte Configurações avançadas/Verificações)*
- ***/SHUTDOWN*** Desligar o computador na conclusão da verificação
- ***/FORCESHUTDOWN*** Forçar o computador a ser desligado na conclusão da verificação
- ***/ADS*** *Verificar fluxos de dados alternativos (apenas NTFS)*
- ***/ARCBOMBSW*** Informar arquivos compactados novamente

11.5. Programação de verificação

Com o **AVG Internet Security 2012**, é possível executar uma verificação sob demanda (por exemplo, quando você suspeitar de uma infecção no seu computador) ou com base em um plano programado. É altamente recomendável executar verificações com base em uma programação. Dessa forma, você pode assegurar que seu computador esteja protegido contra a possibilidade de infecção e não precisará se preocupar com a inicialização da verificação.

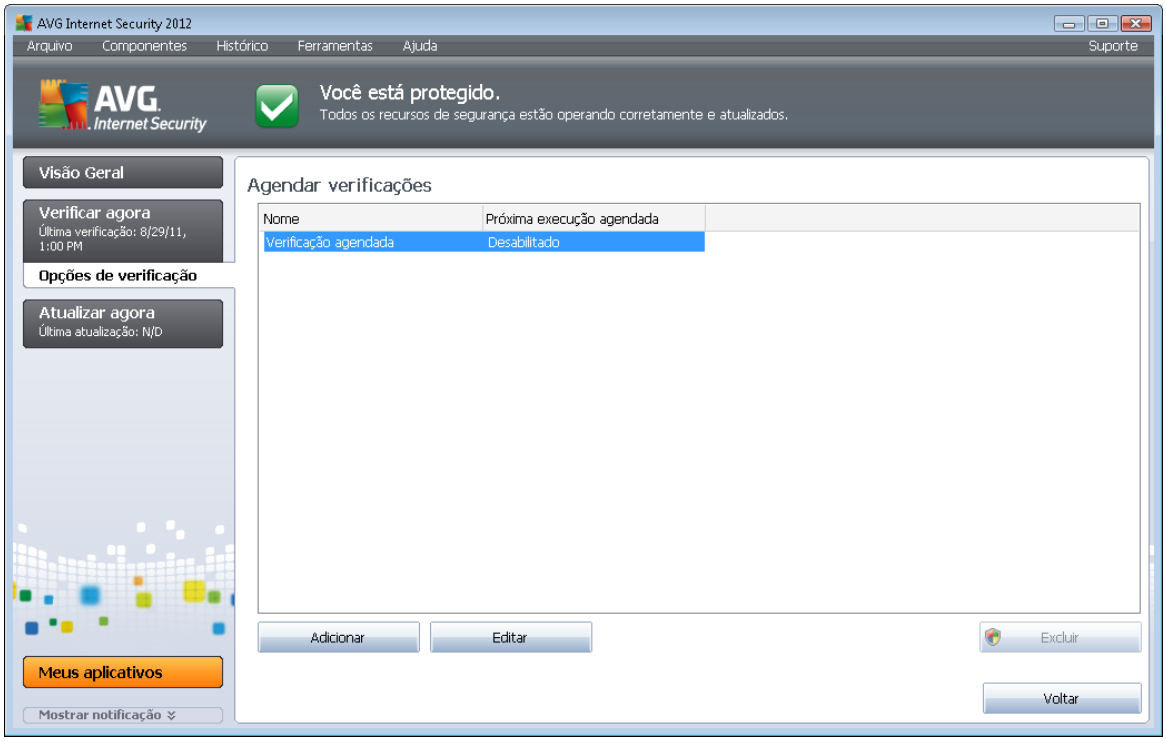
Você deve Verificar todo o computador regularmente, pelo menos uma vez por semana. Mas, se possível, inicie a verificação de todo o computador diariamente, conforme definido na configuração padrão da programação da verificação. Se o computador estiver "sempre ligado", você poderá programar verificações fora dos horários de trabalho. Se o computador for desligado algumas vezes, programe verificações para a inicialização do computador quando a tarefa tiver sido executada.

Para criar novas programações de verificação, consulte a interface de verificação do AVG e localize a seção ***Programar verificações*** , na parte inferior:



Programar verificações

Clique no ícone gráfico na seção ***Programar verificações*** para abrir uma nova caixa de diálogo ***Programar verificações***, na qual você encontrará uma lista de todas as verificações atualmente programadas:

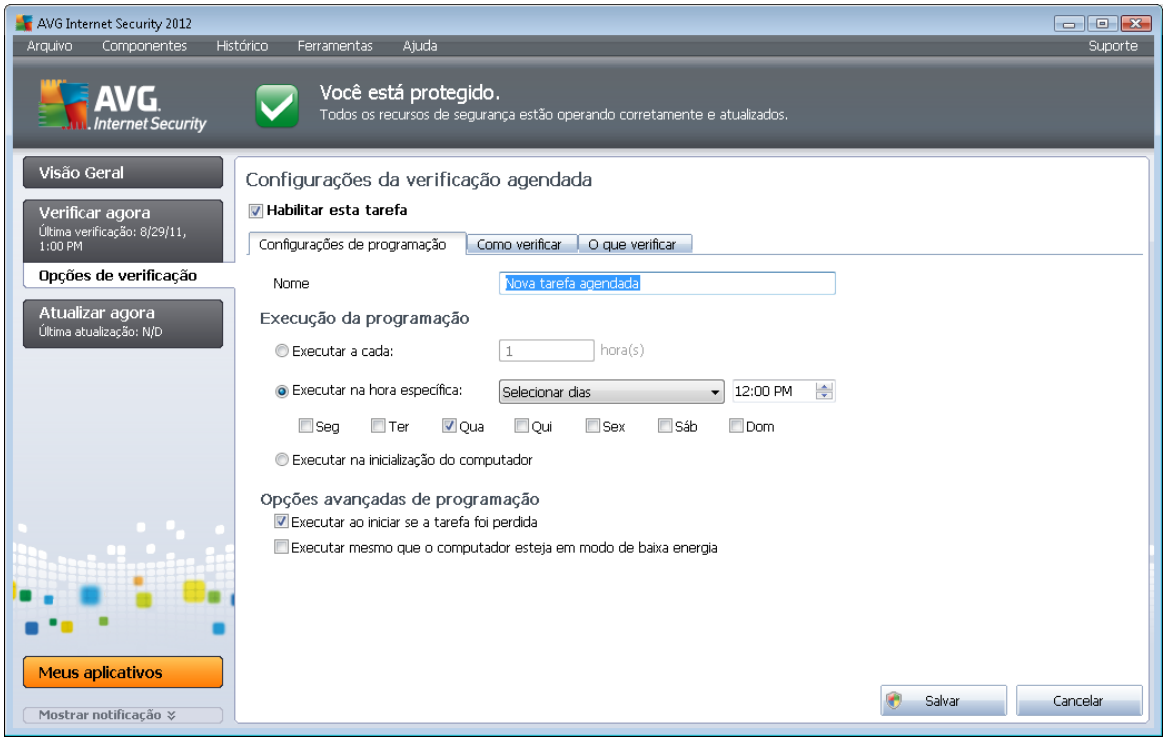


É possível editar/adicionar verificações usando os seguintes botões de controle:

- ***Adicionar programação de verificação*** - o botão abre a caixa de diálogo***Configurações da verificação programada***, guia Configurações de programação. Nessa caixa de diálogo, você pode especificar os parâmetros do teste definido recentemente.
- ***Editar programação de verificação*** - esse botão só pode ser usado se você tiver selecionado um teste existente anteriormente na lista de testes programados. Nesse caso, o botão aparecerá ativo e você poderá clicar nele para passar para a caixa de diálogo ***Configurações da verificação programada*** , guia Configurações de programação. Os parâmetros do teste selecionado já estão especificados e poderão ser editados aqui.
- ***Excluir programação de verificação*** - esse botão também ficará ativo se você tiver selecionado um teste existente anteriormente na lista de testes programados. Esse teste pode ser excluído da lista se você pressionar o botão de controle. Entretanto, você só poderá remover os próprios testes. O teste ***Programação de verificação de todo o computador*** predefinido com as configurações padrão nunca poderá ser excluído.
- ***Voltar*** - retornar à interface de verificação do AVG

11.5.1. Configurações de programação

Se quiser programar um novo teste e sua ativação regular, insira informações na caixa de diálogo ***Configurações para teste programado*** (*clique no botão* ***Adicionar verificação programada*** *na caixa de diálogo* ***Programar verificações***). A caixa de diálogo é dividida em três guias: ***Configurações de programação*** *(veja a imagem abaixo; a guia padrão à qual você será automaticamente redirecionado*), Como verificar e O que verificar.



Na guia ***Configurações de agendamento***, você pode primeiro marcar/desmarcar o item ***Habilitar esta tarefa*** para simplesmente desativar temporariamente o teste programado e ativá-lo novamente conforme necessário.

Em seguida, informe o nome da verificação que você está prestes a criar e agendar. Digite o nome no campo de texto, no item ***Nome***. Tente usar nomes curtos, descritivos e apropriados para a verificação para tornar seu reconhecimento mais fácil posteriormente.

Exemplo: *não é apropriado denominar a verificação como "Nova verificação" ou "Minha verificação", pois esses nomes não se referem exatamente ao que será verificado. Por outro lado, um exemplo de nome descritivo ideal seria "Verificação de áreas do sistema" etc. Além disso, não é necessário especificar no nome da verificação se ela é uma verificação de todo o computador ou somente uma verificação de pastas ou arquivos selecionados. Suas verificações serão sempre uma versão específica da verificação de arquivos ou pastas selecionados.*

Nessa caixa de diálogo você ainda poderá definir os seguintes parâmetros de verificação:

- ***Execução do programa*** - especifica os intervalos de tempo para a inicialização de novas verificações programadas. O tempo pode ser definido pela repetição da inicialização da verificação depois de um determinado período (***Executar a cada ...***) pela definição de uma data e hora exatas (***Executar em uma hora específica...***), ou pela definição de um evento ao qual a inicialização da atualização deve ser associada (***Ação baseada na inicialização do computador***).

- ***Opções de programa avançadas*** - essa seção permite definir sob quais condições a verificação deverá ou não ser inicializada se o computador estiver no modo de pouca energia ou completamente desligado.

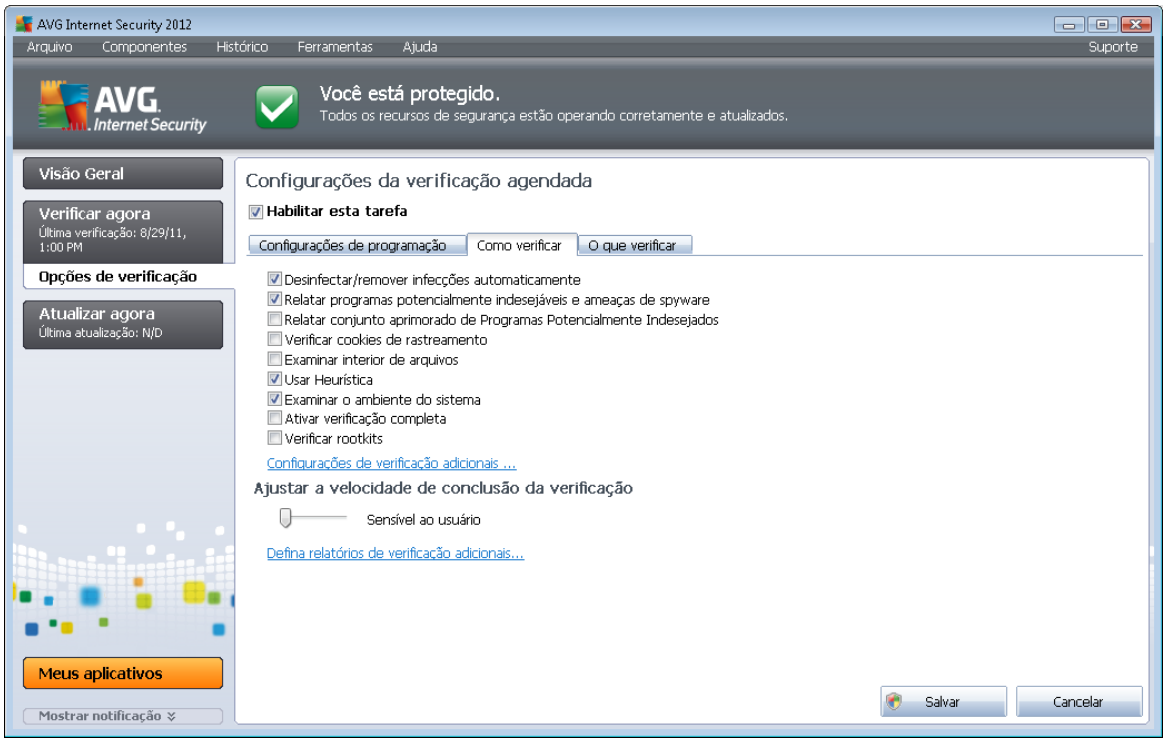
Botões de controle da caixa de diálogo Configurações para verificação programada

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação programada*** *(Configurações de programação, Como verificar e O que verificar)*, e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG. Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG.

11.5.2. Como verificar



Na guia ***Como verificar*** , você encontrará uma lista de parâmetros de verificação que podem ser ativados ou desativados. Por padrão, a maioria dos parâmetros é ativada e a funcionalidade será aplicada durante a verificação. A menos que você tenha um motivo válido para alterar as configurações, recomendamos manter a configuração predefinida:

- ***Reparar ou remover vírus automaticamente*** (*ativada por padrão*): se um vírus for identificado durante a verificação, ele pode ser reparado automaticamente, se houver solução disponível. Caso não seja possível reparar o arquivo infectado automaticamente ou se você decidir desativar essa opção, você será notificado das detecções de vírus e terá que decidir o que fazer com a infecção de vírus detectada. A ação recomendada é remover

o arquivo infectado para a Quarentena de vírus.

- ***Informar programas potencialmente indesejáveis e ameaças de spyware –*** marque para ativar o mecanismo Anti-Spyware e verificar spyware, bem como vírus. Spyware representa uma categoria de malware questionável: embora ele geralmente represente um risco de segurança, alguns desses programas pode ser instalado intencionalmente. Recomendamos manter esse recurso ativado, pois aumenta a segurança do computador.

- ***Informar conjunto avançado de programas potencialmente indesejáveis*** (*desativada por padrão*): marque para detectar o pacote estendido de spyware: programas que estão perfeitamente ok e são inofensivos quando adquiridos do fabricante diretamente, mas podem ser mal-utilizados para finalidades mal-intencionadas posteriormente. Esta é uma medida adicional que aumenta ainda mais a segurança de seu computador; no entanto, pode eventualmente bloquear programas legais, e, portanto, é desativada por padrão.

- ***Verificar cookies de rastreamento*** (*desativada por padrão*): este parâmetro do componente Anti-Spyware define que os cookies devem ser detectados durante a verificação (*cookies HTTP são usados para autenticar, controlar e manter informações específicas sobre usuários, como preferências de sites ou conteúdo de carrinhos de compras eletrônicas*).

- ***Verificar interior dos arquivos*** (*desativada por padrão*): esse parâmetro define que a verificação deve atuar em todos os arquivos, mesmo se eles estiverem compactados em algum tipo de arquivo, como ZIP, RAR etc.

- ***Usar Heurística*** (*ativada por padrão*): a análise heurística (*emulação dinâmica das instruções do objeto verificado, em um ambiente de computador virtual*) será um dos métodos usados para detecção de vírus durante a verificação.

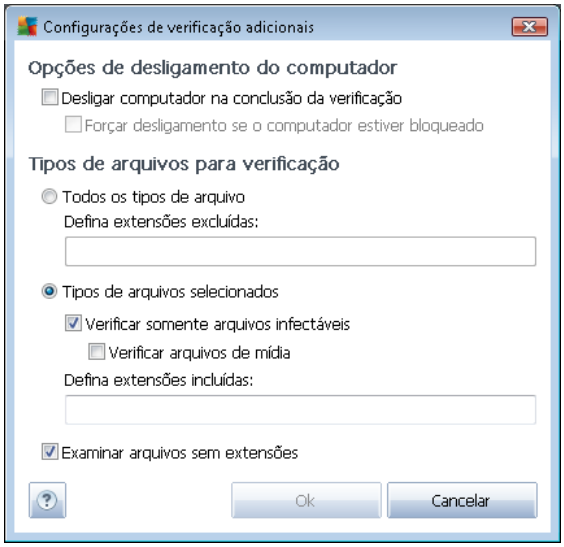
- ***Verificar ambiente do sistema*** (*ativada por padrão*): a verificação também atuará nas áreas do sistema do seu computador.

- ***Ativar verificação completa*** (*desativada por padrão*) - em situações específicas (*suspeita de que seu computador foi infectado*), é possível marcar esta opção para ativar a maioria dos algoritmos de verificação completos que verificarão até mesmo as áreas do computador que dificilmente são infectadas, só para ter a absoluta certeza. Entretanto, lembre-se de que esse método consome bastante tempo.

- ***Verificar rootkits*** (*desativada por padrão*): marque este item se desejar incluir a detecção de rootkit na verificação de todo o computador. A detecção de rootkit também está disponível por meio do componente Anti-Rootkit.

Em seguida, será possível alterar a configuração da verificação da seguinte maneira:

- ***Configurações de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Configurações de verificação adicionais***, na qual é possível especificar os seguintes parâmetros:



- ***Opções de desligamento do computador*** - decida se o computador deve ser desligado automaticamente quando a execução do processo de verificação terminar. Ao confirmar essa opção (***Desligar o computador quando o processo de verificação for concluído***), uma nova opção permitirá que o computador seja desligado mesmo que ele esteja bloqueado (***Forçar desligamento do computador se estiver bloqueado***).

- ***Tipos de arquivo para verificação*** - você deve decidir se deseja verificar os seguintes itens:

  - ***Todos os tipos de arquivos*** com a possibilidade de definirem exceções a partir da verificação, fornecendo uma lista de extensões de arquivo separadas por vírgula que não devem ser verificadas;

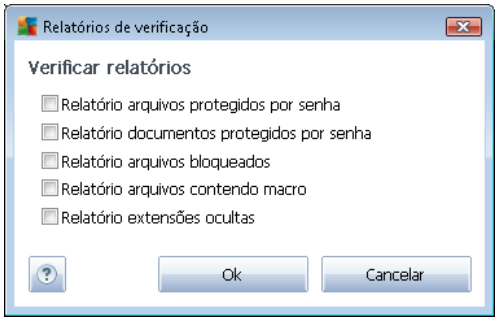
  - ***Tipos de arquivos selecionados*** - você pode especificar que deseja verificar apenas os arquivos possivelmente infectáveis (*arquivos que não podem ser infectados não serão verificados; por exemplo, alguns arquivos de texto simples ou outros arquivos não executáveis*), incluindo arquivos de mídia (*arquivos de áudio e vídeo - se você deixar essa caixa desmarcada, o tempo de verificação será ainda menor, pois esses arquivos costumam ser grandes, e é muito improvável que eles sejam infectados por vírus*). Mais uma vez, é possível especificar por extensões quais são os arquivos que sempre devem ser verificados.

  - Opcionalmente, você pode optar por ***Verificar arquivos sem extensão*** - essa opção está ativada por padrão, e convém mantê-la nesse estado, a não ser que você tenha um motivo concreto para alterá-la. Arquivos sem extensão são relativamente suspeitos e devem ser verificados sempre.

- ***Ajustar a velocidade de conclusão da verificação*** - você pode usar este controle deslizante para alterar a prioridade do processo de verificação. Por padrão, o valor dessa opção é definido no nível *Sensível ao usuário* de uso automático do recurso. Se desejar, você pode executar o processo de verificação em nível mais baixo, fazendo com que o

carregamento dos recursos do sistema seja minimizado (*procedimento útil quando for necessário trabalhar no computador sem se preocupar com o tempo que o sistema usará para fazer a verificação*), ou mais rápido, com maior necessidade de recursos (*por exemplo, quando o computador fica ocioso temporariamente*).

- ***Definir relatórios de verificação adicionais*** - o link abre uma nova caixa de diálogo ***Verificar relatórios*** que permite selecionar quais os possíveis tipos de descobertas devem ser relatados:



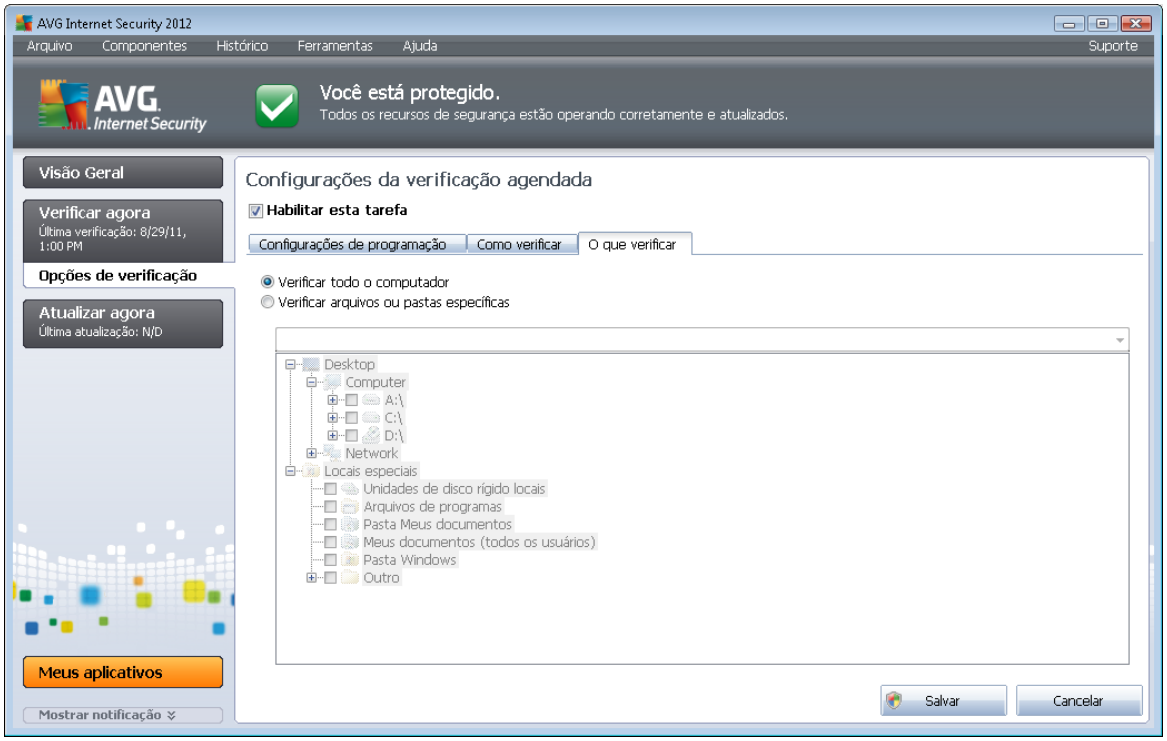
Botões de controle

Há dois botões de controle disponíveis nas três guias da caixa de diálogo ***Configurações da verificação agendada*** (*Configurações de programação, Como verificar* e *O que verificar*) e eles têm a mesma funcionalidade, independentemente da guia em que você esteja no momento:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG. Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.

- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG.

11.5.3. O que verificar



Na guia ***O que verificar***, você pode definir se deseja programar a verificação de todo o computador ou a verificação de arquivos ou pastas específicas.

Se você selecionar a verificação de arquivos ou pastas específicas, na parte inferior dessa caixa de diálogo a estrutura de árvore exibida será ativada e você poderá especificar as pastas para verificação (expanda os itens clicando no nó de mais até encontrar a pasta que deseja verificar). Você pode selecionar várias pastas marcando as respectivas caixas. As pastas selecionadas aparecerão no campo de texto na parte superior da caixa de diálogo e o menu suspenso manterá o histórico das verificações selecionadas para um uso posterior. *Ou você pode inserir o caminho inteiro para a pasta desejada manualmente (se inserir vários caminhos, será necessário separar com pontos-e-vírgulas sem espaços extras*).

Na estrutura de árvore você também pode ver um ramo chamado ***Locais especiais***. A seguir encontre uma lista de locais que serão verificados uma vez que a respectiva caixa de seleção esteja marcada:

- ***Discos rígidos locais*** - todos os discos rígidos de seu computador
- ***Arquivos de programas***
  - C:\Arquivos de Programas\
  - *na versão de 64 bits* C:\Arquivos de Programas (x86)
- ***Pasta Meus documentos***

- *para Windows XP:* C:\Documents and Settings\Usuário padrão\Meus documentos\
- *para Windows Vista/7*: C:\Usuários\usuário\Documentos\

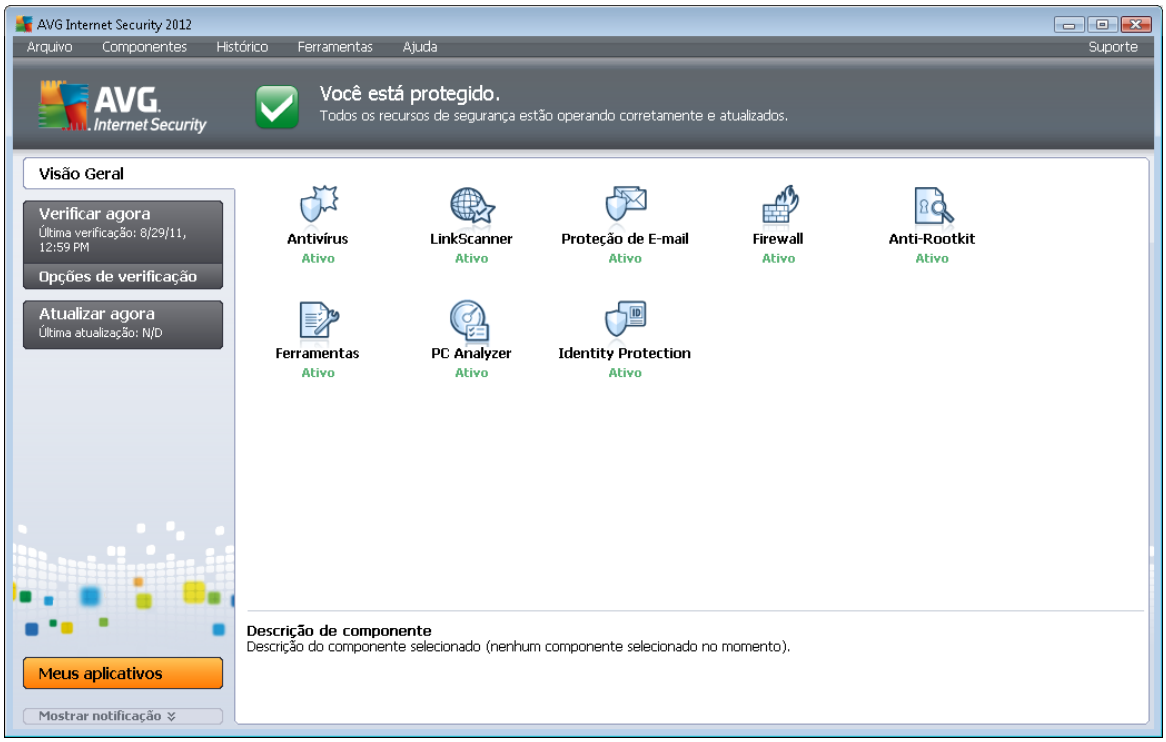
- ***Meus documentos (todos os usuários)***
  - *para Windows XP*: C:\Documents and Settings\Todos os usuários\Documentos\
  - *para Windows Vista/7*: C:\Usuários\Público\Documentos\
- ***Pasta do Windows*** - C:\Windows\
- ***Outro***
  - Drive de sistema – o disco rígido no qual o sistema operacional está instalado (normalmente C:)
  - *Pasta do sistema* - C:\Windows\System32\
  - *Pasta Arquivos Temporários* - C:\Documents and Settings\Usuário\Local\ (*Windows XP*); ou C:\Usuários\usuário\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Arquivos Temporários de Internet* - C:\Documents and Settings\Usuário\Configurações locais\Arquivos temporários de Internet\ (*Windows XP*); ou C:\Usuários\usuário\AppData\Local\Microsoft\Windows\Arquivos Temporários de Internet (*Windows Vista/7*)

Botões de controle

Esses dois botões de controle estão disponíveis em todas as três guias da caixa de diálogo ***Configurações de verificação agendada*** *(Configurações de programação, Como verificar e O que verificar)*:

- ***Salvar*** - salva todas as alterações realizadas nessa guia ou em qualquer outra dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface de verificação do AVG . Portanto, se você desejar configurar os parâmetros de teste em todas as guias, pressione o botão para salvá-los somente depois de ter especificado todos os requisitos.
- ***Cancelar*** - cancela todas as alterações realizadas nessa guia ou em qualquer outra guia dessa caixa de diálogo e volta para a caixa de diálogo padrão da interface do AVG .

11.6. Visão geral dos resultados da verificação



A caixa de diálogo ***Visão geral dos resultados de verificação*** pode ser acessada da interface de verificação do AVG, por meio do botão ***Histórico de verificação***. A caixa de diálogo fornece uma lista de todas as verificações inicializadas anteriormente e as informações sobre seus resultados:

- ***Nome*** - designação da verificação; pode ser o nome de uma das verificações predefinidas ou o nome que você tenha dado à verificação que programou. Todos os nomes incluem um ícone indicando o resultado da verificação:

  - o ícone verde informa que não foram detectadas infecções durante a verificação

  - o ícone azul indica que uma infecção foi detectada durante a verificação, mas o objeto infectado foi removido automaticamente

  - o ícone vermelho avisa que uma infecção foi detectada durante a verificação e não foi possível removê-la!

  Cada ícone pode ser sólido ou cortado ao meio. O ícone sólido indica uma verificação que foi concluída adequadamente. O ícone cortado ao meio indica que a verificação foi cancelada ou interrompida.

  Nota: *para obter informações detalhadas sobre cada verificação, consulte a caixa de diálogo Resultados da Verificação, que pode ser acessada pelo botão Exibir detalhes (na parte inferior desta caixa de diálogo).*

- ***Horário de início*** - a data e a hora em que a verificação foi inicializada

- ***Horário de término*** - a data e a hora em que a verificação foi encerrada
- ***Objetos testados*** - número de objetos que foram verificados
- ***Infecções*** - número de infecções por vírus detectadas/removidas
- ***Spyware*** - número de spyware detectados/removidos
- ***Aviso*** - número de objetos suspeitos detectados
- ***Rootkits*** - número de rootkits detectados rootkits
- ***Informações do log de verificação*** - informações relacionadas ao processo e o resultado da verificação (geralmente em sua finalização ou interrupção)

Botões de controle

Os botões de controle da caixa de diálogo ***Visão geral dos resultados da verificação*** são:

- ***Exibir detalhes***- pressione-o para ativar a caixa de diálogo Resultados da verificação para exibir dados detalhados na verificação selecionada
- ***Excluir resultado*** - pressione-o para remover o item selecionado a partir da visão geral dos resultados da verificação
- ***Voltar*** - volta para a caixa de diálogo padrão da interface de verificação do AVG

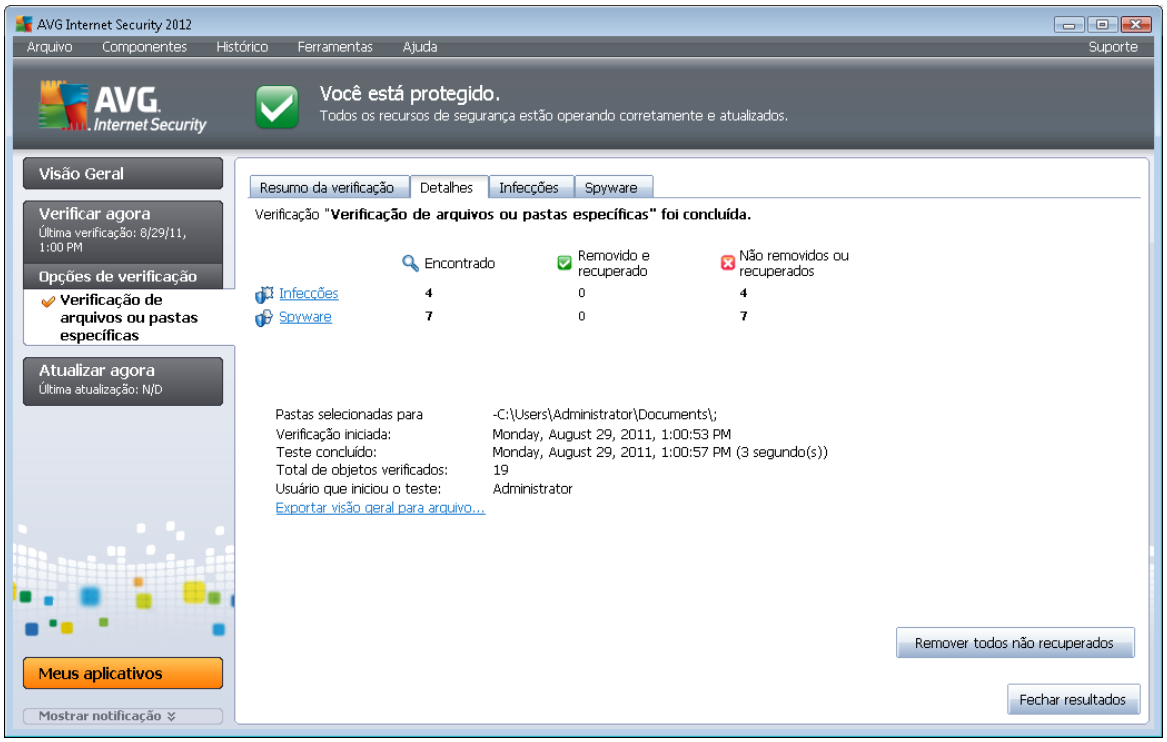
11.7. Detalhes dos resultados da verificação

Se na caixa de diálogo Visão Geral dos Resultados da Verificação uma verificação específica for selecionada, você poderá clicar no botão ***Exibir detalhes*** para passar para a caixa de diálogo ***Resultados da Verificação***, que fornece detalhes sobre o processo e o resultado da verificação selecionada. A caixa de diálogo divide-se em várias guias:

- Visão Geral dos Resultados - essa guia é exibida sempre e fornece dados estatísticos descrevendo o processo de verificação.
- Infecções - essa guia é exibida somente se uma infecção por vírus tiver sido detectada durante a verificação
- Spyware - essa guia é exibida somente se um spyware tiver sido detectado durante a verificação
- Aviso - essa guia é exibida somente se cookies forem detectados durante a verificação
- Rootkits - essa guia é exibida somente se rootkits tiverem sido detectados durante a verificação
- Informações - essa guia é exibida somente se algumas ameaças potenciais tiverem sido detectadas, mas se não tiver sido possível classificá-las em nenhuma das categorias

acima. A guia fornecerá uma mensagem de aviso sobre a descoberta. Além disso, você encontrará aqui informações sobre objetos que não podem ser verificados *(por exemplo, arquivos protegidos por senha)*.

11.7.1. Guia Visão geral dos resultados



Na guia ***Verificar resultados***, é possível encontrar estatísticas detalhadas com informações sobre:

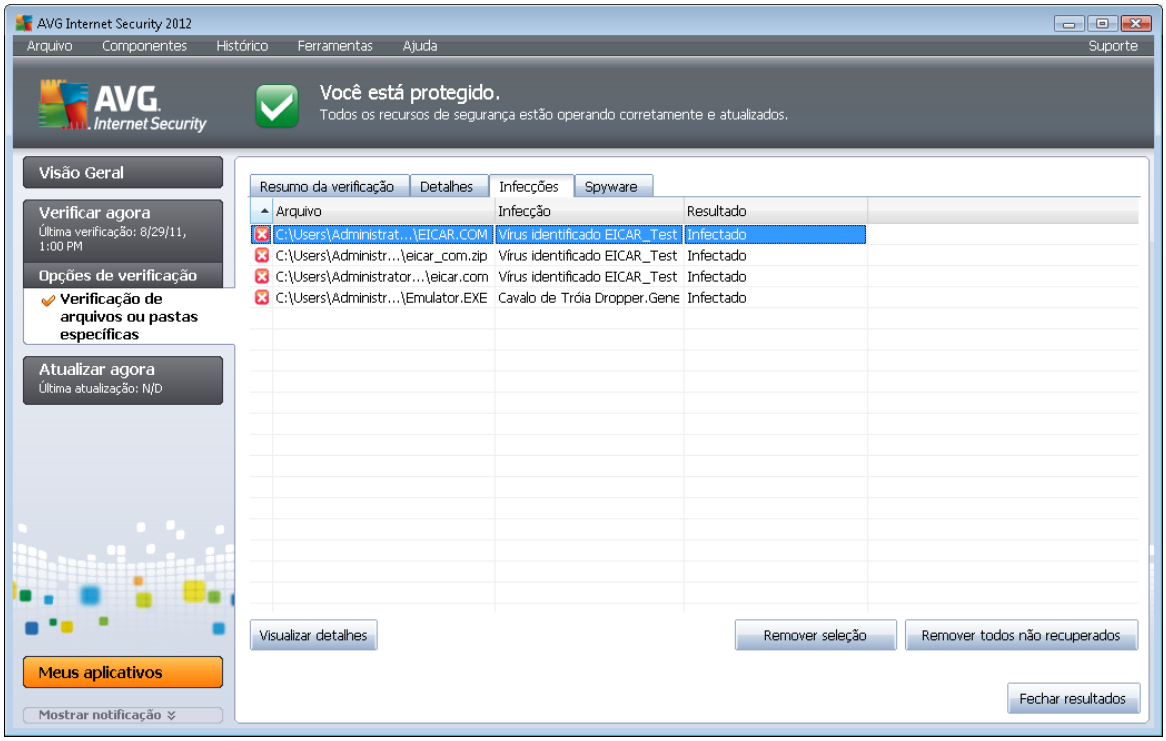
- infecções por vírus/spyware detectadas
- infecções por vírus/spyware removidas
- o número de infecções por vírus/spyware que não puderam ser removidas ou reparadas

Além disso, você encontrará informações sobre a data e a hora exata da inicialização da verificação, o número total de objetos verificados, a duração da verificação e o número de erros ocorridos durante a verificação.

Botões de controle

Há somente um botão de controle disponível nessa caixa de diálogo. O botão ***Fechar resultados*** o leva de volta à caixa de diálogo Visão geral dos resultados da verificação.

11.7.2. Guia Infecções



A guia ***Infecções*** só será exibida na caixa de diálogo ***Resultados da verificação*** se uma infecção de vírus for detectada durante uma verificação. A guia é dividida em três seções, que apresentam estas informações:

- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do vírus detectado (*para obter detalhes sobre o vírus específico, consulte a Enciclopédia de vírus online*).
- ***Resultado*** - define o status atual do objeto infectado detectado durante a verificação.
    - ***Infectado*** - o objeto infectado foi detectado e mantido no local original (*por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica*).
    - ***Reparado*** - o objeto infectado foi reparado automaticamente e mantido no local original
    - ***Movido para Quarentena de Vírus*** - o objeto infectado foi movido para a Quarentena de vírus.
    - ***Excluído*** - o objeto infectado foi excluído.
    - ***Adicionado a extensões PPI*** - a detecção foi avaliada como exceção e adicionada à lista de exceções PPI *(configurada na caixa de diálogo Exceções PPI das*

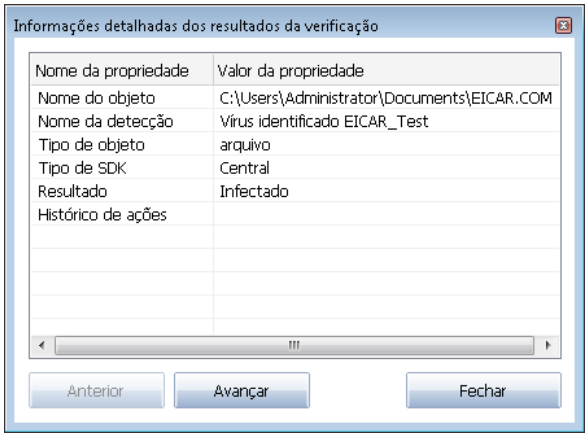
configurações avançadas)

- ***Arquivo bloqueado - não testado*** - o objeto é bloqueado e o AVG não pode verificá-lo.
- ***Objeto potecialmente perigoso*** - o objeto foi detectado como potencialmente perigoso, mas não infectado (ele pode conter macros, por exemplo*)*. As informações devem ser consideradas apenas como aviso.
- ***Reinicialização necessária para concluir ação*** - não é possível remover o objeto infectado. Para removê-lo completamente, é necessário reiniciar o computador.

Botões de controle

Há três botões de controle disponíveis nessa caixa de diálogo:

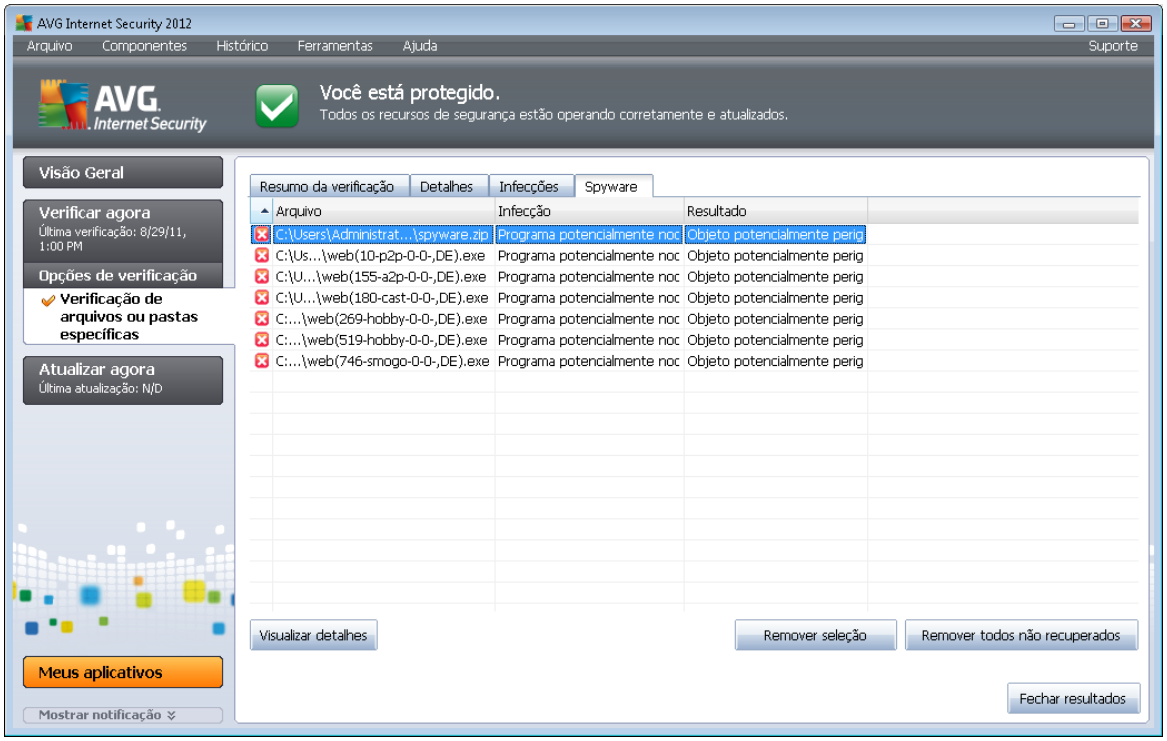
- ***Exibir detalhes*** - o botão abre uma nova janela de diálogo denominada ***Informações detalhadas do objeto***:



  Nesta caixa de diálogo, você pode encontrar informações detalhadas sobre o objeto infeccioso selecionado (*por exemplo, nome e local do objeto infeccioso, tipo de objeto, tipo de SDK, resultado da detecção e histórico de ações relacionado ao objeto detectado*). Usando os botões ***Voltar***/***Avançar***, você pode ver informações sobre descobertas específicas. Use o botão ***Fechar*** para fechar a caixa de diálogo.

- ***Remover selecionadas*** - use o botão para mover a descoberta selecionada para a Quarentena
- ***Remover todas as não reparadas*** - esse botão exclui todas as descobertas de vírus que não foram reparadas ou movidas para a Quarentena
- ***Fechar resultados*** - fecha a visão geral das informações e volta para a caixa de diálogo Visão geral dos resultados da verificação.

11.7.3. Guia Spyware



A guia ***Spyware*** só é exibida na caixa de diálogo ***Verificar resultados*** se um spyware for detectado durante uma verificação. A guia é dividida em três seções, que apresentam estas informações:

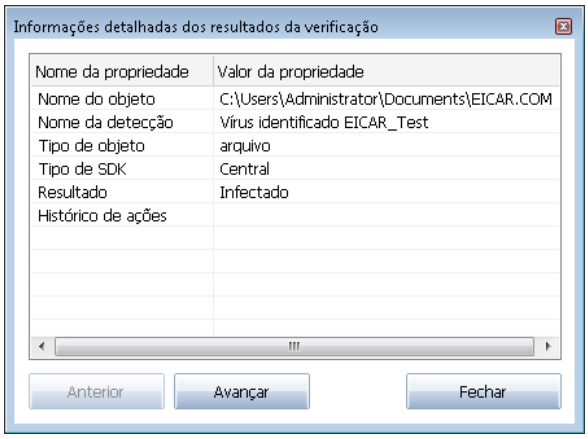
- ***Arquivo*** - caminho completo para o local original do objeto infectado
- ***Infecções*** - nome do spyware detectado *(para obter detalhes sobre vírus específicos, consulte a Enciclopédia de Vírus online)*
- ***Resultado*** - define o status atual do objeto detectado durante a verificação.
    - ***Infectado*** *- o objeto infectado foi detectado e mantido no local original (por exemplo, se você tiver desativado a opção de reparação automática em uma configuração de verificação específica).*
    - ***Reparado*** - o objeto infectado foi reparado automaticamente e mantido no local original
    - ***Movido para Quarentena de Vírus*** - o objeto infectado foi movido para a Quarentena de vírus.
    - ***Excluído*** - o objeto infectado foi excluído.
    - ***Adicionado a extensões PPI*** - a detecção foi avaliada como exceção e adicionada à lista de exceções PPI *(configurada na caixa de diálogo Exceções PPI das configurações avançadas)*

- ***Arquivo bloqueado - não testado*** - o objeto é bloqueado e o AVG não pode verificá-lo.
- ***Objeto potencialmente perigoso***- o objeto foi detectado como potencialmente perigoso, mas não infectado (ele pode conter macros, por exemplo). As informações devem ser consideradas apenas um aviso.
- ***Reinicialização necessária para concluir ação*** - não é possível remover o objeto infectado. Para removê-lo completamente, é necessário reiniciar o computador.

Botões de controle

Há três botões de controle disponíveis nessa caixa de diálogo:

- ***Exibir detalhes*** - o botão abre uma nova janela de diálogo denominada ***Informações detalhadas do objeto***:



  Nesta caixa de diálogo, você pode encontrar informações detalhadas sobre o objeto infeccioso selecionado (*por exemplo, nome e local do objeto infeccioso, tipo de objeto, tipo de SDK, resultado da detecção e histórico de ações relacionado ao objeto detectado*). Usando os botões ***Voltar***/***Avançar***, você pode ver informações sobre descobertas específicas. Use o botão ***Fechar*** para sair da caixa de diálogo.

- ***Remover selecionadas*** - use o botão para mover a descoberta selecionada para a Quarentena
- ***Remover todas as não reparadas*** - esse botão exclui todas as descobertas de vírus que não foram reparadas ou movidas para a Quarentena
- ***Fechar resultados*** - fecha a visão geral das informações e volta para a caixa de diálogo Visão geral dos resultados da verificação.

11.7.4. Guia Avisos

A guia ***Avisos*** exibe informações sobre objetos "suspeitos" (*normalmente arquivos*) detectados durante a verificação. Quando detectados pela Proteção Residente, esses arquivos têm o acesso bloqueado. Exemplos típicos desse tipo de descoberta são: arquivos ocultos, cookies, chaves de Registro suspeitas, documentos ou arquivos protegidos por senha etc Tais arquivos não representam uma ameaça direta para o seu computador ou para a sua segurança. Informações sobre esses arquivos costumam ser úteis no caso de ser detectado um adware ou spyware no seu computador. Se, nos resultados do teste, o **AVG Internet Security 2012** detectar apenas avisos, nenhuma ação será necessária.

Esta é uma breve descrição dos exemplos mais comuns de tais objetos:

- ***Arquivos ocultos*** - por padrão, arquivos ocultos não são visíveis no Windows, e alguns vírus ou outras ameaças podem tentar evitar sua detecção armazenando seus arquivos com esse atributo. Se o **AVG Internet Security 2012** detectar um arquivo oculto que você suspeita ser mal-intencionado, você poderá movê-lo para a Quarentena de vírus.
- ***Cookies*** - cookies são arquivos de texto não-formatado usados em sites para armazenar informações específicas do usuário, usadas posteriormente para carregar o layout personalizado do site, preencher o nome do usuário etc.
- ***Chaves do registro suspeitas*** - certos tipos de malware armazenam suas informações no registro do Windows, para garantir o seu carregamento na inicialização ou ampliar seu efeito no sistema operacional.

11.7.5. Guia Rootkits

A guia ***Rootkits*** exibe informações sobre rootkits detectados durante a verificação caso você tenha iniciado a Verificação Anti-Rootkit.

Um rootkit é um programa criado para assumir o controle fundamental de um sistema de computador, sem autorização dos proprietários do sistema e gerentes legítimos. O acesso ao hardware é realmente necessário, pois um rootkit tem o objetivo de executar o controle do sistema operacional executado no hardware. Geralmente, os rootkits atuam para obscurecer sua presença no sistema por meio de subversão ou evasão de mecanismos de segurança padrão do sistema operacional. Freqüentemente, eles também são cavalos-de-tróia, levando os usuários a acreditarem que é confiável executá-los no sistema. As técnicas usadas para conseguir isso podem incluir ocultar processos em execução de programas de monitoramento ou ocultar arquivos ou dados do sistema operacional.

A estrutura dessa guia é basicamente a mesma que a da guia Infecções ou da guia Spyware.

11.7.6. Guia Informações

A guia ***Informações*** contém dados como "descobertas" que não podem ser categorizadas como infecções, spyware etc. Elas também não podem ser rotuladas positivamente como perigosas, mas merecem a sua atenção. A verificação do **AVG Internet Security 2012** é capaz de detectar arquivos que podem não estar infectados, mas que são suspeitos. Esses arquivos são indicados como Aviso ou como Informações.

As ***Informações*** sobre severidade podem ser reportadas por um dos seguintes motivos:

- ***Compactado em tempo de execução*** - o arquivo foi compactado com um dos compactadores menos comuns, o que pode indicar uma tentativa de impedir a verificação desse arquivo. Entretanto, nem todos os relatórios de tal arquivo indica um vírus.

- ***Compactado em tempo de execução com recorrência*** - semelhante ao problema acima, mas menos freqüente entre os softwares comuns. Esses arquivos são suspeitos e convém considerar sua remoção ou envio para análise.

- ***Arquivo ou documento protegido por senha*** - arquivos protegidos por senha não podem ser verificados pelo **AVG Internet Security 2012** (*ou em geral por qualquer outro programa anti-malware*).

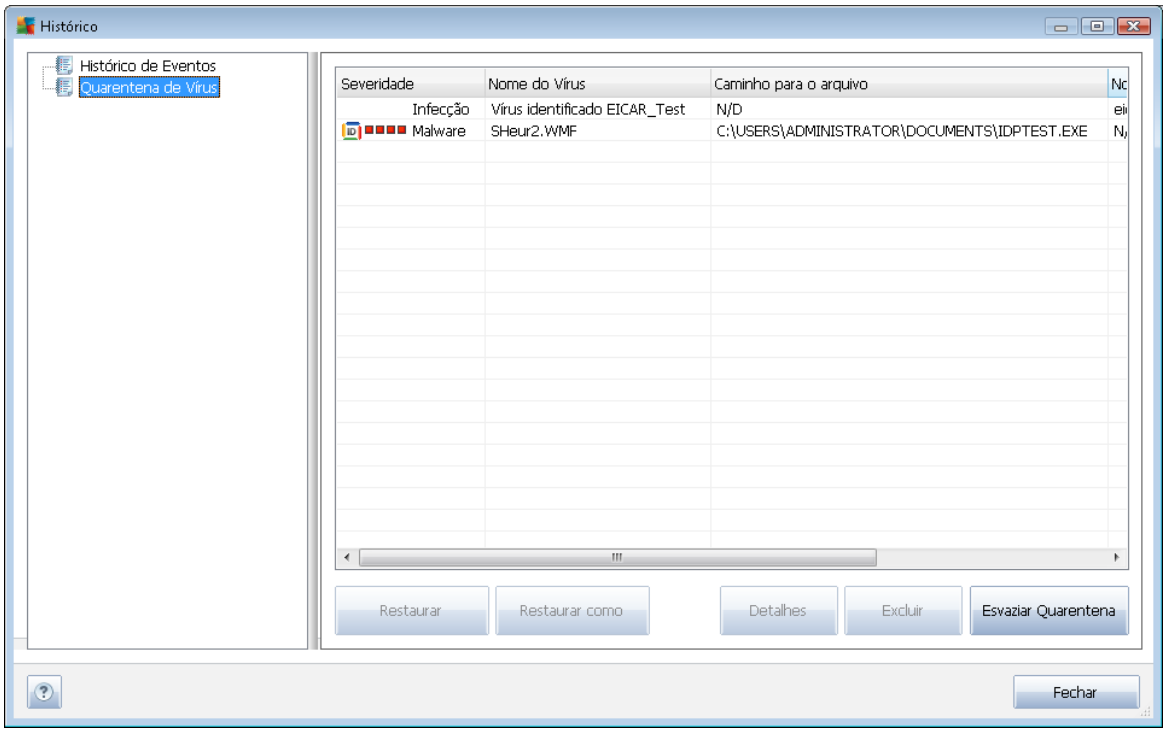
- ***Documento com macros*** - o documento relatado contém macros, que podem ser mal-intencionadas.

- ***Extensão oculta*** - arquivos com extensão oculta podem parecer ser, por exemplo, imagens, quando na verdade são arquivos executáveis (*por exemplo, imagem.jpg.exe*). A segunda extensão não é visível no Windows por padrão, e o **AVG Internet Security 2012** relata esses arquivos para evitar que sejam abertos acidentalmente.

- ***Caminho de arquivo impróprio*** - se algum arquivo do sistema importante estiver em execução a partir de um caminho diferente do padrão (*por exemplo, winlogon.exe em execução a partir de um caminho diferente da pasta Windows*), o irá relatar essa discrepância. **AVG Internet Security 2012** Em alguns casos, vírus usam nomes de processos padrão do sistema para tornar sua presença menos aparente no sistema.

- ***Arquivo bloqueado*** - o arquivo relatado está bloqueado, e por isso não pode ser verificado pelo **AVG Internet Security 2012**. Isso normalmente significa que algum arquivo é&; constantemente utilizado pelo sistema (*por exemplo, arquivo swap*).

11.8. Quarentena de vírus



A Quarentena de vírus é um ambiente seguro para o gerenciamento de objetos suspeitos ou infectados detectados durante os testes do AVG. Depois que um objeto infectado for detectado durante a verificação e o AVG não puder repará-lo automaticamente, você será solicitado a decidir o que deve ser feito com o objeto suspeito. A solução recomendável é movê-lo para a ***Quarentena de Vírus*** para futuro tratamento. O principal objetivo da Quarentena de Vírus é conservar qualquer arquivo excluído por um certo período de tempo para que você tenha certeza de que não precisa mais dele em seu local original. Se você descobrir que a ausência de arquivos causa problemas, pode enviar o arquivo em questão para análise ou restaurá-lo para o local original.

A interface da ***Quarentena de Vírus*** é aberta em uma janela separada e oferece uma visão geral das informações de objetos infectados em quarentena:

- ***Severidade*** caso você decida instalar o componente Identity Protection **AVG Internet Security 2012**no seu, uma identificação gráfica da respectiva severidade da descoberta, em uma escala de quatro níveis que varia desde incensurável (□□□□) até muito perigosa (■■■■) será fornecida nesta seção; e as informações sobre o tipo de infecção*com base em seu nível de infecção - todos os objetos listados podem estar positivamente ou potencialmente infectados.*

- ***Nome do vírus*** - especifica o nome da infecção detectada de acordo com a Enciclopédia de vírus *(online)*

- ***Caminho para o arquivo*** - caminho completo para o local original do arquivo infectado detectado

- ***Nome original do objeto*** - todos os objetos detectados listados na tabela foram rotulados com o nome padrão dado pelo AVG durante o processo de verificação. No caso de o objeto ter tido um nome original que é conhecido (*por ex., o nome de um anexo de e-mail que não corresponda ao conteúdo real do anexo*), ele será fornecido nesta coluna.

- ***Data do armazenamento*** - data e hora que o arquivo suspeito foi detectado e armazenado na Quarentena de vírus

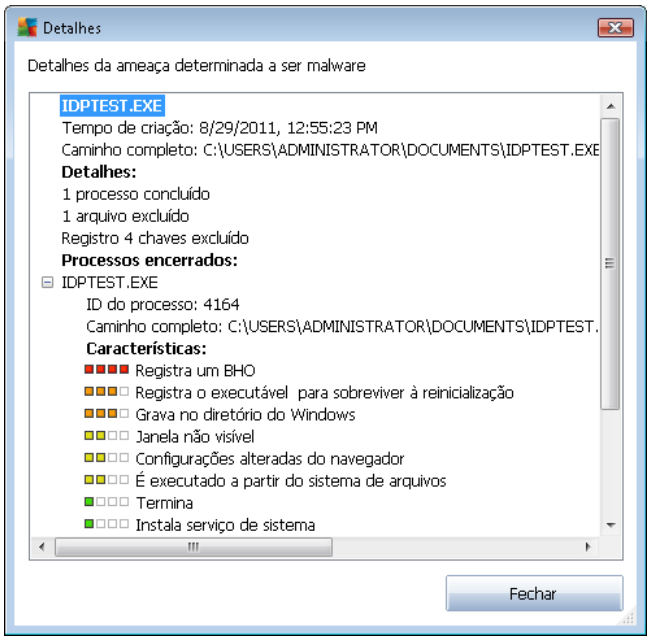
Botões de controle

Os botões de controle a seguir podem ser acessados na interface da ***Quarentena de vírus***:

- ***Restaurar*** - remove o arquivo infectado de volta ao local original do disco

- ***Restaurar como*** – move o arquivo infectado para a pasta selecionada

- ***Detalhes*** – esse botão aplica-se apenas às ameaças detectadas pelo Identity Protection. Ao clicar, exibe uma visão geral sinótica dos detalhes da ameaça (quais arquivos/ processos foram afetados, características do processo, etc.). Observe que para todos os outros itens que não sejam detectados pelo IDP, esse botão fica esmaecido e inativo!



- ***Excluir*** - remove de maneira completa e irreversível o arquivo infectado da ***Quarentena***

- ***Esvaziar a Quarentena*** - remove completamente todo o conteúdo da ***Quarentena de Vírus*** Removendo os arquivos da ***Quarentena***, esses arquivos serão removidos de modo irreversível do disco (*e não para a Lixeira*).

12. Atualizações do AVG

Nenhum software de segurança pode garantir proteção real de vários tipos de ameaças se não for regularmente atualizado! Os criadores de vírus estão sempre em busca de novas brechas que possam explorar em softwares e sistemas operacionais. Novos vírus, novos malwares, novos ataques de hackers surgem diariamente. Por esse motivo, os fornecedores de software estão continuamente emitindo atualizações e patches de segurança para corrigir qualquer brecha de segurança que seja descoberta.

Considerando todas as ameaças ao computador recentemente descobertas e a velocidade com que se disseminam, é absolutamente crucial atualizar o **AVG Internet Security 2012** com regularidade. A melhor solução é ater-se às configurações padrão do programa onde a atualização automática está configurada. Se o banco de dados de vírus de seu **AVG Internet Security 2012** não estiver atualizado, o programa não poderá detectar as ameaças mais recentes!

É fundamental atualizar o AVG regularmente! As atualizações das definições de vírus essenciais devem ser feitas diariamente, se possível. Atualizações de programas menos urgentes podem ser feitas semanalmente.

12.1. Iniciar atualização

Para proporcionar o máximo de segurança disponível, o **AVG Internet Security 2012** é programado para verificar se há novas atualizações a cada quatro horas. Como as atualizações do AVG não são lançadas de acordo com uma programação fixa, mas de acordo com a quantidade e severidade de novas ameaças, essa verificação é altamente importante para garantir que o banco de dados de vírus do seu AVG fique atualizado o tempo todo.

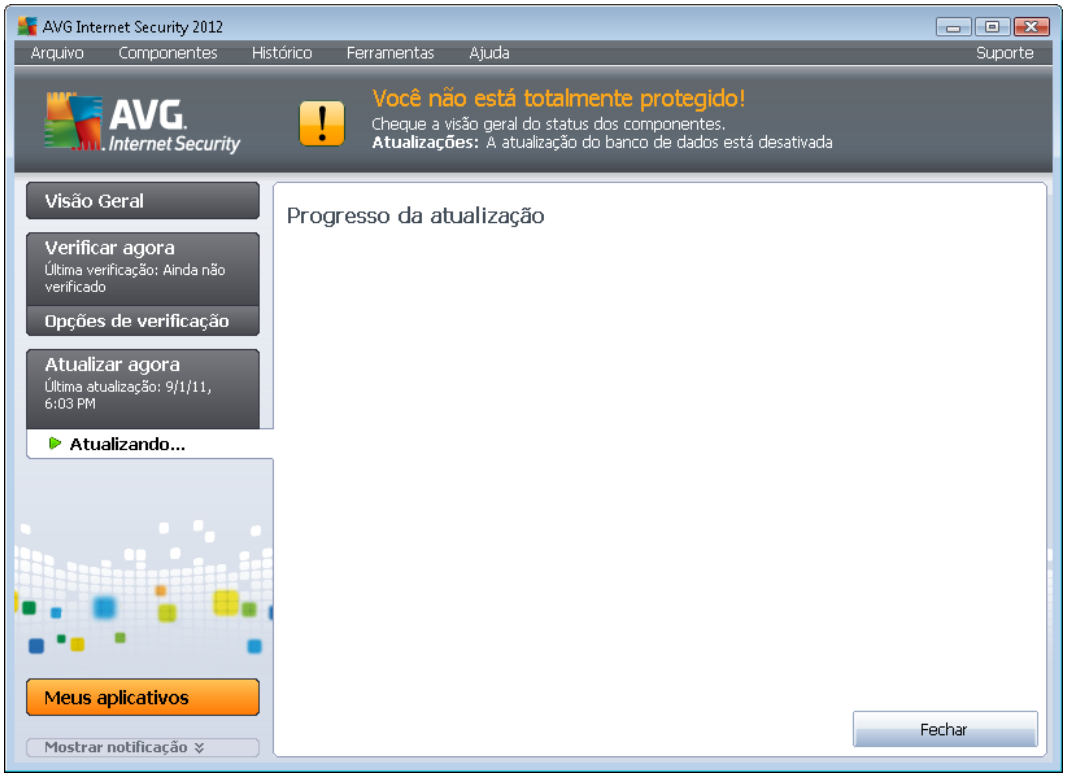
Se desejar reduzir a frequência das atualizações, você poderá configurar seus próprios parâmetros de inicialização. No entanto, é altamente recomendável executar a atualização, pelo menos, uma vez ao dia. A configuração pode ser editada na seção Configurações avançadas/Programações, especificamente nas seguintes caixas de diálogo:

- Agendamento de atualização de definições
- Agendamento de atualização de programa
- Agendamento de atualização do Anti-Spam

Para verificar se há novos arquivos de atualização imediatamente, use o link rápido Atualizar agora, na interface de usuário principal. Esse link está sempre disponível em qualquer caixa de diálogo da interface de usuário.

12.2. Progresso da atualização

Quando você inicia a atualização, o AVG primeiro verifica se há novos arquivos de atualização disponíveis. Se houver, o **AVG Internet Security 2012** iniciará o download e executará o processo de atualização. Durante o processo de atualização, você será redirecionado para a interface ***Atualizar***, onde poderá ver o andamento do processo em uma representação gráfica, bem como obter uma visão geral dos parâmetros estatísticos relevantes (*tamanho do arquivo de atualização, dados recebidos, velocidade de download, tempo decorrido etc.*):



***Nota**: antes do início de cada atualização do programa AVG, é criado um ponto de restauração do sistema. No caso de falha no processo de atualização e no sistema operacional, sempre é possível restaurar seu sistema operacional para a configuração original a partir desse ponto. Essa opção está disponível no menu do Windows em: Iniciar/Todos os Programas/ Acessórios/Ferramentas do Sistema/Restauração do Sistema. Recomendado apenas para usuários experientes!*

12.3. Níveis de atualização

O **AVG Internet Security 2012** oferece dois níveis de atualização:

- ***A atualização de definições*** contém as alterações necessárias para a proteção antivírus, anti-spam e anti-malware confiável. Em geral, não inclui nenhuma alteração no código e atualiza apenas o banco de dados de definições. Essa atualização deverá ser aplicada assim que estiver disponível.

- ***A atualização do programa*** contém várias alterações, correções e aperfeiçoamentos para o programa.

Ao agendar uma atualização, você pode definir parâmetros específicos para ambos os níveis de atualização:

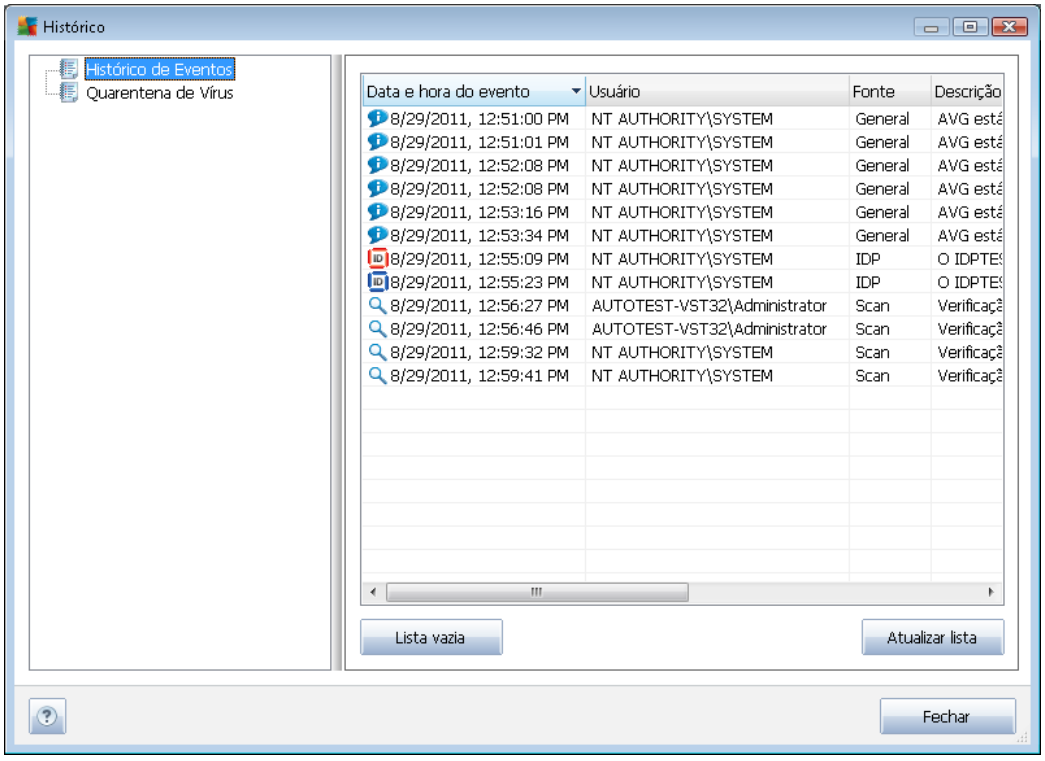
- Agendamento de atualização de definições

- Agendamento de atualização de programa

***Observação:** se ocorrer uma coincidência de tempo de uma atualização de programa agendada e*

uma verificação agendada, o processo de atualização terá maior prioridade, e a verificação será interrompida.

13. Histórico de Eventos



A caixa de diálogo ***Histórico*** pode ser acessada no menu do sistema por meio do item ***Histórico/ Log do Histórico de Eventos***. Nesta caixa de diálogo, você encontrará um resumo dos eventos importantes que ocorreram durante a operação do AVG Internet Security 2012. ***Histórico*** registra os seguintes tipos de eventos:

- Informações sobre atualizações do aplicativo AVG
- Informações no início, no fim ou na interrupção da verificação (*inclusive testes executados automaticamente*)
- Informações sobre eventos associados à detecção de vírus (*pela Proteção Residente ou verificação*), incluindo o local de ocorrência
- Outros eventos importantes

Para cada evento, as seguintes informações são listadas:

- ***Data e hora do evento*** fornece a data e a hora exata em que o evento ocorreu
- ***O campo Usuário*** informa o nome do usuário conectado no momento em que ocorreu o evento
- ***O campo Origem*** fornece informações sobre o componente de origem ou outra parte do sistema AVG que acionou o evento

- ***Descrição do evento*** fornece um breve resumo do que realmente aconteceu

Botões de controle

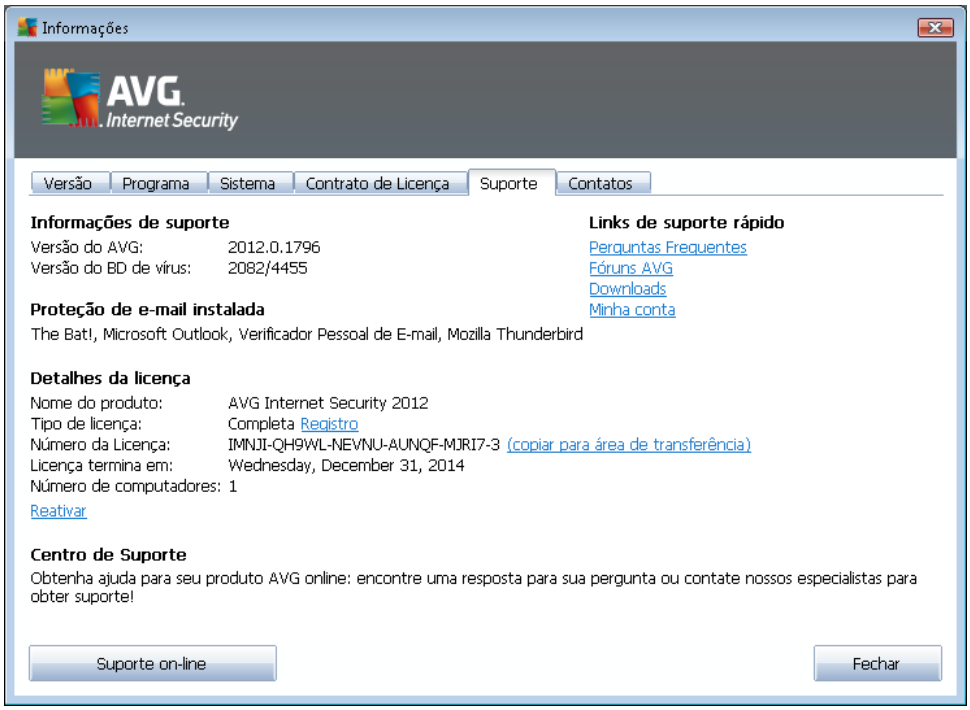
- ***Esvaziar lista***- clique no botão para excluir todas as entradas na lista de eventos
- ***Atualizar lista***- clique no botão para atualizar todas as entradas na lista de eventos

14. Perguntas Freqüentes e Suporte Técnico

Caso tenha problemas técnicos ou relacionados a vendas com o aplicativo **AVG Internet Security 2012**, há várias maneiras de obter ajuda. Selecione entre as opções abaixo:

- ***Entrar em contato com o suporte ao cliente***: dentro do aplicativo AVG, você pode entrar em contato com nosso suporte profissional ao cliente. Selecione o item do menu principal ***Ajuda /Obter ajuda online*** para ser redirecionado ao formulário de contato online para comunicar-se com o suporte ao cliente, disponível 24 horas por dia, 7 dias da semana. O número de sua licença será preenchido automaticamente. Para prosseguir, siga as instruções na página da Web.

- ***Suporte (link no menu principal)***: o menu do aplicativo AVG (*na parte superior da interface de usuário principal*) inclui o link ***Suporte*** que abre uma nova caixa de diálogo com todos os tipos de informações de que você precisa enquanto obtém ajuda. A caixa de diálogo inclui dados básicos sobre o programa AVG instalado (*versão do banco de dados/ programa*), detalhes da licença e uma lista de links rápidos de suporte:



- ***Solução de problemas no arquivo de ajuda***: uma nova seção de ***Solução de problemas*** é disponibilizada diretamente no arquivo de ajuda incluído no **AVG Internet Security 2012**. Esta seção fornece uma lista das situações mais frequentes quando um usuário deseja buscar ajuda profissional para um problema técnico. Selecione a situação que melhor descreve seu problema e clique nela para abrir instruções detalhadas que levem a solucionar o problema.

- ***Centro de Suporte do site do AVG***: como alternativa, você pode buscar a solução de problemas no site do AVG(http://www.avg.com/). Na seção ***Centro de Suporte***, você pode encontrar uma visão geral estruturada sobre grupos temáticos que lidam com problemas técnicos e relacionados a vendas.

- ***Perguntas frequentes***: no site do AVG (http://www.avg.com/) você também pode encontrar uma seção separada e de estrutura elaborada com perguntas frequentes. Esta seção pode ser acessada pela opção de menu ***Centro de Suporte/Perguntas frequentes***. Novamente, todas as perguntas são divididas de maneira organizada nas categorias técnica, de vendas e de vírus.

- ***Sobre vírus e ameaças***: um capítulo específico do site do AVG (http://www.avg.com/) é dedicado aos problemas com vírus. No menu, selecione ***Centro de Suporte/Sobre vírus e ameaças*** para acessar uma página com uma visão geral estruturada das informações relacionadas a ameaças online. Você também pode encontrar instruções sobre a remoção de vírus, spyware e dicas sobre como permanecer protegido.

- ***Fórum de discussões***: você também pode usar o fórum de discussões de usuários do AVG em http://forums.avg.com.